ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.01 Основы защиты АИС

Направление подготовки 10.03.01 Информационная безопасность

Профиль образовательной программы *Безопасность автоматизированных систем*

Форма обучения *очная*

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция № 1-2 (4 часа).

Тема: «Основные понятия, термины и определения»

1.1.1 Вопросы лекции:

1. Введение в проблемы информационной безопасности.
2. Основные понятия, термины и определения.

…….

1.1.2 Краткое содержание вопросов:

1. Введение в проблемы информационной безопасности.

- Что такое информационная безопасность.
- Уровни решения проблемы информационной безопасности.
- Содержание основных законов Российской Федерации в сфере компьютерного права.
- Уровни защиты информации.
- Меры защиты информационной безопасности.
- Угрозы для информационной безопасности, связанные с подключением к глобальной компьютерной сети Интернет и меры безопасного использования сервисов Интернета.

В связи с массовой информатизацией современного общества все большую актуальность приобретает знание нравственно-этических норм и правовых основ использования средств новых информационных технологий в повседневной практической деятельности. Наглядными примерами, иллюстрирующими необходимость защиты информации и обеспечения информационной безопасности, являются участившиеся сообщения о компьютерных «взломах» банков, росте компьютерного пиратства, распространении компьютерных вирусов.

Число компьютерных преступлений растет, также увеличиваются масштабы компьютерных злоупотреблений. Умышленные компьютерные преступления составляют заметную часть преступлений, но злоупотреблений компьютерами и ошибок еще больше.

Основной причиной потерь, связанных с компьютерами, является недостаточная образованность в области безопасности.

Под информационной безопасностью понимается защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации.

Цель информационной безопасности - обезопасить ценности системы, защитить и гарантировать точность и целостность информации и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена.

На практике важнейшими являются три аспекта информационной безопасности:

- доступность (возможность за разумное время получить требуемую информационную услугу);

- целостность (ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения).

Кроме того, использование информационных систем должно производиться в соответствии с существующим законодательством. Данное положение, разумеется, применимо к любому виду деятельности, однако информационные технологии специфичны в том отношении, что развиваются исключительно быстрыми темпами. Почти всегда законодательство отстает от потребностей практики, и это создает в обществе определенную напряженность. Для информационных технологий подобное отставание законов, нормативных актов, национальных и отраслевых стандартов оказывается особенно болезненным.

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно разделить на четыре уровня:

1. законодательный (законы, нормативные акты, стандарты и т.п.);
2. административный (действия общего характера, предпринимаемые руководством организации);
3. процедурный (конкретные меры безопасности, имеющие дело с людьми);
4. программно-технический (конкретные технические меры).

2. Основные понятия, термины и определения.

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

- конфиденциальность (англ. *confidentiality*) — состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право;
- целостность (англ. *integrity*) — избежание несанкционированной модификации информации;
- доступность (англ. *availability*) — избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

- неотказуемость или апеллируемость (англ. *non-repudiation*) — способность удостоверять имевшее место действие или событие так, что эти события или действия не могли быть позже отвергнуты;
- подотчётность (англ. *accountability*) — свойство, обеспечивающее однозначное прослеживание действий любого логического объекта.;
- достоверность (англ. *reliability*) — свойство соответствия предусмотренному поведению или результату;
- аутентичность или подлинность (англ. *authenticity*) — свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Системный подход к описанию информационной безопасности предлагает выделить следующие составляющие информационной безопасности[9]:

1. Законодательная, нормативно-правовая и научная база.
2. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
3. Организационно-технические и режимные меры и методы (Политика информационной безопасности).
4. Программно-технические способы и средства обеспечения информационной безопасности.

Ниже в данном разделе подробно будет рассмотрена каждая из составляющих информационной безопасности.

Целью реализации информационной безопасности какого-либо объекта является построение Системы обеспечения информационной безопасности данного объекта (СОИБ). Для построения и эффективной эксплуатации СОИБ необходимо[3]:

- выявить требования защиты информации, специфические для данного объекта защиты;
- учесть требования национального и международного Законодательства;
- использовать наработанные практики (стандарты, методологии) построения подобных СОИБ;
- определить подразделения, ответственные за реализацию и поддержку СОИБ;
- распределить между подразделениями области ответственности в осуществлении требований СОИБ;
- на базе управления рисками информационной безопасности определить общие положения, технические и организационные требования, составляющие Политику информационной безопасности объекта защиты;
- реализовать требования Политики информационной безопасности, внедрив соответствующие программно-технические способы и средства защиты информации;
- реализовать Систему менеджмента (управления) информационной безопасности (СМИБ);
- используя СМИБ организовать регулярный контроль эффективности СОИБ и при необходимости пересмотр и корректировку СОИБ и СМИБ.

Как видно из последнего этапа работ, процесс реализации СОИБ непрерывный и циклично (после каждого пересмотра) возвращается к первому этапу, повторяя последовательно все остальные. Так СОИБ корректируется для эффективного выполнения своих задач защиты информации и соответствия новым требованиям постоянно обновляющейся информационной системы.

…….

1. 2 Лекция № 3 (2 часа).

Тема: «Основы государственной политики в области информационной безопасности»

1.2.1 Вопросы лекции:

1. Основы государственной политики в области информационной безопасности.
2. Стратегия национальной безопасности Российской Федерации.

…….

1.2.2 Краткое содержание вопросов:

1. Основы государственной политики в области информационной безопасности.

1. Настоящие Основы являются документом стратегического планирования Российской Федерации.

2. Настоящими Основами определяются основные угрозы в области международной информационной безопасности, цель, задачи и приоритетные направления государственной политики Российской Федерации в области международной информационной безопасности (далее - государственная политика Российской Федерации), а также механизмы их реализации.

3. Нормативную правовую базу настоящих Основ составляют Конституция Российской Федерации, международные договоры Российской Федерации в области международной информационной безопасности, федеральные законы, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, иные нормативные правовые акты Российской Федерации.

4. Настоящие Основы конкретизируют отдельные положения Стратегии национальной безопасности Российской Федерации до 2020 года, Доктрины информационной безопасности Российской Федерации, Концепции внешней политики Российской Федерации и других документов стратегического планирования Российской Федерации.

5. Настоящие Основы предназначены:

а) для продвижения на международной арене российских инициатив в области формирования системы международной информационной безопасности, включая совершенствование правового, организационного и иных видов ее обеспечения;

б) для формирования межгосударственных целевых программ в области международной информационной безопасности, в осуществлении которых участвует Российская Федерация, а также государственных и федеральных целевых программ в данной области;

в) для организации межведомственного взаимодействия при реализации государственной политики Российской Федерации в области международной информационной безопасности;

г) для достижения и поддержания технологического паритета с ведущими мировыми державами за счет более широкого использования информационных и коммуникационных технологий в реальном секторе экономики.

6. Под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

7. Под системой международной информационной безопасности понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства. Система международной информационной безопасности призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве. Сотрудничество в области формирования системы международной информационной

безопасности отвечает национальным интересам Российской Федерации и способствует укреплению ее национальной безопасности.

8. Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

II. Цель и задачи государственной политики Российской Федерации

9. Цель государственной политики Российской Федерации заключается в содействии установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности.

10. Достижению цели государственной политики Российской Федерации будет способствовать участие Российской Федерации в решении следующих задач:

а) формирование системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях;

б) создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

в) формирование механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях;

г) создание условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств;

д) повышение эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий;

е) создание условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами.

III. Основные направления государственной политики Российской Федерации

11. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях, являются:

а) создание условий для продвижения на международной арене российской инициативы в необходимости разработки и принятия государствами - членами Организации Объединенных Наций Конвенции об обеспечении международной информационной

безопасности;
б) содействие закреплению российских инициатив в области формирования системы международной информационной безопасности в итоговых документах, изданных по результатам работы Группы правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также содействие выработке под эгидой Организации Объединенных Наций правил поведения в области обеспечения международной информационной безопасности, отвечающих национальным интересам Российской Федерации;
в) проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и планов действий с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС, странами - членами Азиатско-тихоокеанского экономического сотрудничества, странами - членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами в области международной информационной безопасности;
г) продвижение на международной арене российской инициативы в интернационализации управления информационно-телекоммуникационной сетью «Интернет» и увеличение в этом контексте роли Международного союза электросвязи;
д) организационно-штатное укрепление структурных подразделений федеральных органов исполнительной власти, участвующих в реализации государственной политики Российской Федерации, а также совершенствование координации деятельности федеральных органов исполнительной власти в данной области;
е) создание механизма участия российского экспертного сообщества в совершенствовании аналитического и научно-методического обеспечения продвижения российских инициатив в области формирования системы международной информационной безопасности;
ж) создание условий для заключения между Российской Федерацией и иностранными государствами международных договоров о сотрудничестве в области обеспечения международной информационной безопасности;
з) усиление взаимодействия в рамках Соглашения между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности и содействие расширению состава участников указанного Соглашения;
и) использование научного, исследовательского и экспертного потенциала Организации Объединенных Наций, других международных организаций для продвижения российских инициатив в области формирования системы международной информационной безопасности.
12. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий, способствующих снижению риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности, являются:
а) развитие диалога с заинтересованными государствами о национальных подходах к противодействию вызовам и угрозам, возникающим в связи с масштабным использованием информационных и коммуникационных технологий в военно-политических целях;
б) участие в выработке на двустороннем и многостороннем уровнях мер по укреплению доверия в области противодействия угрозам использования информационных и коммуникационных технологий для осуществления враждебных действий и актов

агрессии;
в) содействие развитию региональных систем и формированию глобальной системы международной информационной безопасности на основе общепризнанных принципов и норм международного права (уважение государственного суверенитета, невмешательство во внутренние дела других государств, неприменение силы и угрозы силой в международных отношениях, право на индивидуальную и коллективную самооборону, уважение прав и основных свобод человека);
г) содействие подготовке и принятию государствами - членами Организации Объединенных Наций международных правовых актов, регламентирующих применение принципов и норм международного гуманитарного права в сфере использования информационных и коммуникационных технологий;
д) создание условий для установления международного правового режима нераспространения информационного оружия.
13. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях, являются:
а) развитие сотрудничества с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС, способствующего предупреждению, выявлению, пресечению, раскрытию и расследованию актов деструктивного воздействия на элементы национальной критической информационной инфраструктуры, минимизации последствий реализации таких актов, а также противодействию использования информационно-телекоммуникационной сети «Интернет» и других информационно-телекоммуникационных сетей в целях пропаганды терроризма и привлечения к террористической деятельности новых сторонников;
б) содействие подготовке и принятию государствами - членами Организации Объединенных Наций акта, определяющего порядок обмена информацией о передовых практиках в области обеспечения безопасности функционирования элементов критической информационной инфраструктуры.
14. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств, являются:
а) участие в разработке и реализации межгосударственной системы мер по противодействию указанным угрозам;
б) содействие созданию международного механизма постоянного контроля за недопущением использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств.
15. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по повышению эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий, являются:
а) продвижение на международной арене российской инициативы в необходимости разработки и принятия под эгидой Организации Объединенных Наций Конвенции о сотрудничестве в сфере противодействия информационной преступности, а также активизация работы с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами -

участниками БРИКС по поддержке данной инициативы;
б) развитие сотрудничества в сфере противодействия информационной преступности с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС, странами -членами Азиатско-тихоокеанского экономического сотрудничества, странами - членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами;
в) повышение эффективности информационного обмена между правоохранительными органами государств в ходе расследования преступлений в сфере использования информационных и коммуникационных технологий;
г) совершенствование механизма обмена информацией о методиках расследования и судебной практике рассмотрения дел о преступлениях в сфере использования информационных и коммуникационных технологий.

16. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами, являются:
а) содействие разработке и реализации международных программ, способствующих преодолению информационного неравенства между развитыми и развивающимися странами;
б) содействие развитию национальных информационных инфраструктур и участию государств мирового сообщества в процессах создания и использования глобальных информационных сетей и систем.

IV. Механизмы реализации государственной политики Российской Федерации

17. Государственная политика Российской Федерации реализуется федеральными органами исполнительной власти и надзорными органами в соответствии с предметами их ведения при выполнении соответствующих межгосударственных целевых программ, в осуществлении которых участвует Российская Федерация, государственных и федеральных целевых программ, в том числе в рамках государственно-частного партнерства.

18. Подготовка предложений Президенту Российской Федерации по реализации основных направлений государственной политики Российской Федерации осуществляется рабочими органами Совета Безопасности Российской Федерации во взаимодействии с заинтересованными самостоятельными подразделениями Администрации Президента Российской Федерации, федеральными органами исполнительной власти и организациями.

19. Общая координация деятельности федеральных органов исполнительной власти, связанной с реализацией государственной политики Российской Федерации, а также с продвижением согласованной позиции Российской Федерации по этому вопросу на международной арене, осуществляется Министерством иностранных дел Российской Федерации.

* * *

20. Интенсивное развитие информационных и коммуникационных технологий, их широкое применение во всех сферах деятельности человека создали условия для формирования глобальной информационной инфраструктуры, которая предоставила качественно новые возможности социализации людей, их общения и доступа к накопленным человечеством знаниям.
В современном обществе информационные и коммуникационные технологии являются

основным фактором, определяющим уровень социально-экономического развития и состояние национальной безопасности.
Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года призваны способствовать активизации внешней политики Российской Федерации на пути достижения согласия и учета взаимных интересов в процессе интернационализации глобального информационного пространства.

2. Стратегия национальной безопасности Российской Федерации.

1. Общие положения

1. Настоящая Стратегия является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу.

2. Правовую основу настоящей Стратегии составляют Конституция Российской Федерации, федеральные законы от 28 декабря 2010 г. N 390-ФЗ "О безопасности" и от 28 июня 2014 г. N 172-ФЗ "О стратегическом планировании в Российской Федерации", другие федеральные законы, нормативные правовые акты Президента Российской Федерации.

3. Настоящая Стратегия призвана консолидировать усилия федеральных органов государственной власти, других государственных органов, органов государственной власти субъектов Российской Федерации (далее - органы государственной власти), органов местного самоуправления, институтов гражданского общества по созданию благоприятных внутренних и внешних условий для реализации национальных интересов и стратегических национальных приоритетов Российской Федерации.

4. Настоящая Стратегия является основой для формирования и реализации государственной политики в сфере обеспечения национальной безопасности Российской Федерации.

5. Настоящая Стратегия основана на неразрывной взаимосвязи и взаимозависимости национальной безопасности Российской Федерации и социально-экономического развития страны.

6. В настоящей Стратегии используются следующие основные понятия:

национальная безопасность Российской Федерации (далее - национальная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее - граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности;

национальные интересы Российской Федерации (далее - национальные интересы)

объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития;

угроза национальной безопасности - совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам;

обеспечение национальной безопасности - реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов;

стратегические национальные приоритеты Российской Федерации (далее - стратегические национальные приоритеты) - важнейшие направления обеспечения национальной безопасности;

система обеспечения национальной безопасности совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов государственной власти и органов местного самоуправления и находящихся в их распоряжении инструментов.

II. Россия в современном мире

7. Государственная политика в сфере обеспечения национальной безопасности и социально-экономического развития Российской Федерации способствует реализации стратегических национальных приоритетов и эффективной защите национальных интересов. В настоящее время создана устойчивая основа для дальнейшего наращивания экономического, политического, военного и духовного потенциалов Российской Федерации, повышения ее роли в формирующемся полицентричном мире.

8. Россия продемонстрировала способность к обеспечению суверенитета, независимости, государственной и территориальной целостности, защиты прав соотечественников за рубежом. Возросла роль Российской Федерации в решении важнейших международных проблем, урегулировании военных конфликтов, обеспечении стратегической стабильности и верховенства международного права в межгосударственных отношениях.

9. Экономика России проявила способность к сохранению и укреплению своего потенциала в условиях нестабильности мировой экономики и применения ограничительных экономических мер, введенных рядом стран против Российской Федерации.

10. Позитивные тенденции наметились в решении задач укрепления здоровья граждан. Отмечаются естественный прирост населения, увеличение средней продолжительности жизни.

11. Возрождаются традиционные российские духовно-нравственные ценности. У подрастающего поколения формируется достойное отношение к истории России. Происходит консолидация гражданского общества вокруг общих ценностей, формирующих фундамент государственности, таких как свобода и независимость

России, гуманизм, межнациональный мир и согласие, единство культур многонационального народа Российской Федерации, уважение семейных и конфессиональных традиций, патриотизм.

12. Укрепление России происходит на фоне новых угроз национальной безопасности, имеющих комплексный взаимосвязанный характер. Проведение Российской Федерацией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых делах. Реализуемая ими политика сдерживания России предусматривает оказание на нее политического, экономического, военного и информационного давления.

13. Процесс формирования новой полицентричной модели мироустройства сопровождается ростом глобальной и региональной нестабильности. Обостряются противоречия, связанные с неравномерностью мирового развития, углублением разрыва между уровнями благосостояния стран, борьбой за ресурсы, доступом к рынкам сбыта, контролем над транспортными артериями.

Конкуренция между государствами все в большей степени охватывает ценности и модели общественного развития, человеческий, научный и технологический потенциалы. Особое значение в этом процессе приобретает лидерство в освоении ресурсов Мирового океана и Арктики. В борьбе за влияние на международной арене задействован весь спектр политических, финансово-экономических и информационных инструментов. Все активнее используется потенциал специальных служб.

14. В международных отношениях не снижается роль фактора силы. Стремление к наращиванию и модернизации наступательного вооружения, созданию и развертыванию его новых видов ослабляет систему глобальной безопасности, а также систему договоров и соглашений в области контроля над вооружением. В Евро-Атлантическом, Евразийском и Азиатско-Тихоокеанском регионах не соблюдаются принципы равной и неделимой безопасности. В соседних с Россией регионах развиваются процессы милитаризации и гонки вооружений.

15. Наращивание силового потенциала Организации Североатлантического договора (НАТО) и наделение ее глобальными функциями, реализуемыми в нарушение норм международного права, активизация военной деятельности стран блока, дальнейшее расширение альянса, приближение его военной инфраструктуры к российским границам создают угрозу национальной безопасности.

Возможности поддержания глобальной и региональной стабильности существенно снижаются при размещении в Европе, Азиатско-Тихоокеанском регионе и на Ближнем Востоке компонентов системы противоракетной обороны США, в условиях практической реализации концепции "глобального удара", развертывания стратегических неядерных систем высокоточного оружия, а также в случае размещения оружия в космосе.

16. Сохраняющийся блоковый подход к решению международных проблем не способствует противодействию всему спектру современных вызовов и угроз. Активизация миграционных потоков из стран Африки и Ближнего Востока в Европу показала несостоятельность региональной системы безопасности в Евро-Атлантическом регионе, построенной на основе НАТО и Европейского союза.

17. Позиция Запада, направленная на противодействие интеграционным процессам и создание очагов напряженности в Евразийском регионе, оказывает негативное влияние на реализацию российских национальных интересов. Поддержка США и Европейским союзом антиконституционного государственного переворота на Украине привела к глубокому расколу в украинском обществе и возникновению вооруженного конфликта. Укрепление крайне правой националистической идеологии, целенаправленное формирование у украинского населения образа врага в лице России, неприкрытая ставка на силовое решение внутригосударственных противоречий, глубокий социально-экономический кризис превращают Украину в долгосрочный очаг нестабильности в Европе и непосредственно у границ России.

18. Практика свержения легитимных политических режимов, провоцирования внутригосударственных нестабильности и конфликтов получает все более широкое распространение. Наряду с сохраняющимися очагами напряженности на Ближнем и Среднем Востоке, в Африке, Южной Азии, на Корейском полуострове появляются новые "горячие точки", расширяются зоны, не контролируемые властями каких-либо государств. Территории вооруженных конфликтов становятся базой для распространения терроризма, межнациональной розни, религиозной вражды, иных проявлений экстремизма. Появление террористической организации, объявившей себя "Исламским государством", и укрепление ее влияния стали результатом политики двойных стандартов, которой некоторые государства придерживаются в области борьбы с терроризмом.

19. Сохраняется риск увеличения числа стран - обладателей ядерного оружия, распространения и использования химического оружия, а также неопределенность относительно фактов обладания иностранными государствами биологическим оружием, наличия у них потенциала для его разработки и производства. На территориях соседних с Россией государств расширяется сеть военнобиологических лабораторий США.

20. Критическое состояние физической сохранности опасных объектов и материалов, особенно в государствах с нестабильной внутриполитической ситуацией, неконтролируемое распространение обычного вооружения повышают вероятность их попадания в руки террористов.

21. Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории.

22. Появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. Обостряются угрозы, связанные с неконтролируемой и незаконной миграцией, торговлей людьми, наркоторговлей и другими проявлениями транснациональной организованной преступности.

23. Осложняются мировая демографическая ситуация, проблемы окружающей среды и продовольственной безопасности. Более ощутимыми становятся дефицит пресной воды, последствия изменения климата. Получают распространение эпидемии, многие из которых вызваны новыми, неизвестными ранее вирусами.

24. Возрастающее влияние политических факторов на экономические процессы, а также

попытки применения отдельными государствами экономических методов, инструментов финансовой, торговой, инвестиционной и технологической политики для решения своих геополитических задач ослабляют устойчивость системы международных экономических отношений. На фоне структурных дисбалансов в мировой экономике и финансовой системе, растущей суверенной задолженности, волатильности рынка энергоресурсов сохраняется высокий риск повторения масштабных финансово-экономических кризисов.

25. Государства в качестве реакции на рост международной нестабильности все чаще берут на себя ответственность за дела в своих регионах. Региональные и субрегиональные торговые и иные экономические соглашения становятся одним из важнейших средств защиты от кризисных явлений. Повышается интерес к использованию региональных валют.

26. Для предотвращения угроз национальной безопасности Российская Федерация сосредоточивает усилия на укреплении внутреннего единства российского общества, обеспечении социальной стабильности, межнационального согласия и религиозной терпимости, устранении структурных дисбалансов в экономике и ее модернизации, повышении обороноспособности страны.

27. В целях защиты национальных интересов Россия проводит открытую, рациональную и прагматичную внешнюю политику, исключающую затратную конфронтацию (в том числе новую гонку вооружений).

28. Российская Федерация выстраивает международные отношения на принципах международного права, обеспечения надежной и равной безопасности государств, взаимного уважения народов, сохранения многообразия их культур, традиций и интересов. Россия заинтересована в развитии взаимовыгодного и равноправного торгово-экономического сотрудничества с иностранными государствами, является ответственным участником многосторонней торговой системы. Цель Российской Федерации заключается в приобретении как можно большего числа равноправных партнеров в различных частях мира.

29. В области международной безопасности Россия сохраняет приверженность использованию прежде всего политических и правовых инструментов, механизмов дипломатии и миротворчества. Применение военной силы для защиты национальных интересов возможно только в том случае, если все принятые меры ненасильственного характера оказались неэффективными.

III. Национальные интересы и стратегические национальные приоритеты

30. Национальными интересами на долгосрочную перспективу являются:

укрепление обороны страны, обеспечение незыблемости конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации;
укрепление национального согласия, политической и социальной стабильности, развитие демократических институтов, совершенствование механизмов взаимодействия государства и гражданского общества;
повышение качества жизни, укрепление здоровья населения, обеспечение стабильного демографического развития страны;

сохранение и развитие культуры, традиционных российских духовно-нравственных ценностей;
повышение конкурентоспособности национальной экономики;
закрепление за Российской Федерацией статуса одной из лидирующих мировых держав, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях полицентричного мира.

31. Обеспечение национальных интересов осуществляется посредством реализации следующих стратегических национальных приоритетов:

оборона страны;
государственная и общественная безопасность;
повышение качества жизни российских граждан;
экономический рост;
наука, технологии и образование;
здравоохранение;
культура;
экология живых систем и рациональное природопользование;
стратегическая стабильность и равноправное стратегическое партнерство.

IV. Обеспечение национальной безопасности

32. Состояние национальной безопасности напрямую зависит от степени реализации стратегических национальных приоритетов и эффективности функционирования системы обеспечения национальной безопасности.

Оборона страны

33. Стратегическими целями обороны страны являются создание условий для мирного и динамичного социально-экономического развития Российской Федерации, обеспечение ее военной безопасности.

34. Достижение стратегических целей обороны страны осуществляется в рамках реализации военной политики путем стратегического сдерживания и предотвращения военных конфликтов, совершенствования военной организации государства, форм и способов применения Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, повышения мобилизационной готовности Российской Федерации и готовности сил и средств гражданской обороны.

35. Основные положения военной политики и задачи военно-экономического обеспечения обороны страны, военные опасности и военные угрозы определяются Военной доктриной Российской Федерации.

36. В целях обеспечения стратегического сдерживания и предотвращения военных конфликтов разрабатываются и реализуются взаимосвязанные политические, военные, военно-технические, дипломатические, экономические, информационные и иные меры, направленные на предотвращение применения военной силы в отношении России, защиту ее суверенитета и территориальной целостности. Стратегическое сдерживание и предотвращение военных конфликтов осуществляются путем поддержания потенциала ядерного сдерживания на достаточном уровне, а Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов в заданной степени

готовности к боевому применению.

37. Совершенствование военной организации государства осуществляется на основе своевременного выявления существующих и перспективных военных опасностей и военных угроз, сбалансированного развития компонентов военной организации, наращивания оборонного потенциала, оснащения Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов современными вооружением, военной и специальной техникой, инновационного развития оборонно-промышленного комплекса Российской Федерации.

38. Совершенствование форм и способов применения Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов предусматривает своевременный учет тенденций изменения характера современных войн и вооруженных конфликтов, создание условий для наиболее полной реализации боевых возможностей войск (сил), выработку требований к перспективным формированиям и новым средствам вооруженной борьбы.

39. Повышение мобилизационной готовности Российской Федерации осуществляется путем совершенствования планирования мер по обеспечению мобилизационной подготовки и мобилизации в Российской Федерации и их реализации в необходимом объеме, своевременного обновления и поддержания на достаточном уровне военно-технического потенциала военной организации государства. Важнейшими направлениями совершенствования мобилизационной подготовки являются подготовка экономики Российской Федерации, экономики субъектов Российской Федерации, экономики муниципальных образований, подготовка органов государственной власти, органов местного самоуправления и организаций, Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов к выполнению задач в соответствии с их предназначением и удовлетворению потребностей государства и нужд населения в военное время.

40. Готовность сил и средств гражданской обороны обеспечивается заблаговременно путем проведения мероприятий по подготовке к защите и по защите населения, материальных и культурных ценностей на территории Российской Федерации от опасностей, возникающих при военных конфликтах или вследствие этих конфликтов, а также при чрезвычайных ситуациях природного и техногенного характера.

41. Обеспечение обороны страны осуществляется на основании принципов рациональной достаточности и эффективности, в том числе путем применения методов и средств невоенного реагирования, механизмов дипломатии и миротворчества, расширения международного военного и военно-технического сотрудничества, контроля над вооружением и использования других международно-правовых инструментов.

Государственная и общественная безопасность

42. Стратегическими целями государственной и общественной безопасности являются защита конституционного строя, суверенитета, государственной и территориальной целостности Российской Федерации, основных прав и свобод человека и гражданина, сохранение гражданского мира, политической и социальной стабильности в обществе. защита населения и территорий от чрезвычайных ситуаций природного и техногенного характера.

43. Основными угрозами государственной и общественной безопасности являются:

разведывательная и иная деятельность специальных служб и организаций иностранных государств, отдельных лиц, наносящая ущерб национальным интересам;

деятельность террористических и экстремистских организаций, направленная на насильственное изменение конституционного строя Российской Федерации, дестабилизацию работы органов государственной власти, уничтожение или нарушение функционирования военных и промышленных объектов, объектов жизнеобеспечения населения, транспортной инфраструктуры, устрашение населения, в том числе путем завладения оружием массового уничтожения, радиоактивными, отравляющими, токсичными, химически и биологически опасными веществами, совершения актов ядерного терроризма, нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации;

деятельность радикальных общественных объединений и группировок, использующих националистическую и религиозно-экстремистскую идеологию, иностранных и международных неправительственных организаций, финансовых и экономических структур, а также частных лиц, направленная на нарушение единства и территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране, включая инспирирование "цветных революций", разрушение традиционных российских духовно-нравственных ценностей;

деятельность преступных организаций и группировок, в том числе транснациональных, связанная с незаконным оборотом наркотических средств и психотропных веществ, оружия, боеприпасов, взрывчатых веществ, организацией незаконной миграции и торговлей людьми;

деятельность, связанная с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе;

преступные посягательства, направленные против личности, собственности, государственной власти, общественной и экономической безопасности;

коррупция;

стихийные бедствия, аварии и катастрофы, в том числе связанные с глобальным изменением климата, ухудшением технического состояния объектов инфраструктуры и возникновением пожаров.

44. Главными направлениями обеспечения государственной и общественной безопасности являются усиление роли государства в качестве гаранта безопасности личности и прав собственности, совершенствование правового регулирования предупреждения преступности (в том числе в информационной сфере), коррупции, терроризма и экстремизма, распространения наркотиков и борьбы с такими явлениями, развитие взаимодействия органов обеспечения государственной безопасности и правопорядка с гражданским обществом, повышение доверия граждан к правоохранительной и судебной системам Российской Федерации, эффективности защиты прав и законных интересов российских граждан за рубежом, расширение

международного сотрудничества в области государственной и общественной безопасности.

45. Обеспечение государственной и общественной безопасности осуществляется путем повышения эффективности деятельности правоохранительных органов и специальных служб, органов государственного контроля (надзора), совершенствования единой государственной системы профилактики преступности, в первую очередь среди несовершеннолетних, и иных правонарушений (включая мониторинг и оценку эффективности правоприменительной практики), разработки и использования специальных мер, направленных на снижение уровня криминализации общественных отношений.

46. Особое внимание уделяется искоренению причин и условий, порождающих коррупцию, которая является препятствием устойчивому развитию Российской Федерации и реализации стратегических национальных приоритетов. В этих целях реализуются Национальная стратегия противодействия коррупции и национальные планы противодействия коррупции, в обществе формируется атмосфера неприемлемости данного явления, повышается уровень ответственности за коррупционные преступления, совершенствуется правоприменительная практика в указанной области.

47. В целях обеспечения государственной и общественной безопасности:

совершенствуются структура и деятельность федеральных органов исполнительной власти, развивается система выявления, предупреждения и пресечения разведывательной и иной деструктивной деятельности специальных служб и организаций иностранных государств, наносящей ущерб национальным интересам, актов терроризма, проявлений религиозного радикализма, национализма, сепаратизма, иных форм экстремизма, организованной преступности и других преступных посягательств на конституционный строй Российской Федерации, права и свободы человека и гражданина, государственную и частную собственность, общественный порядок и общественную безопасность;

создаются механизмы предупреждения и нейтрализации социальных и межнациональных конфликтов, а также противодействия участию российских граждан в деятельности преступных и террористических группировок за рубежом;

укрепляется режим безопасного функционирования, повышается уровень антитеррористической защищенности организаций оборонно-промышленного, ядерного, химического, топливно-энергетического комплексов страны, объектов жизнеобеспечения населения, транспортной инфраструктуры, других критически важных и потенциально опасных объектов;
совершенствуется система выявления и анализа угроз в информационной сфере, противодействия им;
принимаются меры для повышения защищенности граждан и общества от деструктивного информационного воздействия со стороны экстремистских и террористических организаций, иностранных специальных служб и пропагандистских структур;
осуществляется комплексное развитие правоохранительных органов и специальных служб, укрепляются социальные гарантии их сотрудникам, совершенствуется научно-техническая поддержка правоохранительной деятельности, принимаются на вооружение перспективные специальные средства и техника, развивается система

профессиональной подготовки специалистов в области обеспечения государственной и общественной безопасности;
повышается социальная ответственность органов обеспечения государственной и общественной безопасности.

…….

1. 3 Лекция № 4 (2 часа).

Тема: «Аттестация объектов информатизации по требованиям безопасности информации»

1.3.1 Вопросы лекции:

1. Общие положения.
2. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.
3. Порядок проведения аттестации и контроля.

…….

1.3.2 Краткое содержание вопросов:

1.Общие положения.

1.1. Настоящее Положение устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

1.2. Положение разработано в соответствии с Законами Российской Федерации "О сертификации продукции и услуг" и "О государственной тайне", "Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам", "Положением о государственном лицензировании деятельности в области защиты информации", "Положением о сертификации средств защиты информации по требованиям безопасности информации", "Системой сертификации ГОСТ Р".

1.3. Система аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации) является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном Госстандартом России порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации (далее - федеральный орган по сертификации и аттестации), которым является Гостехкомиссия России.

1.4. Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России.

Наличие на объекте информатизации действующего "Аттестата соответствия" дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в "Аттестате соответствия".

1.5. Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.

В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

1.6. При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

1.7. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

1.8. Аттестация проводится органом по аттестации в установленном настоящим Положением порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;

- предварительное ознакомление с аттестуемым объектом информатизации;

- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;

- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

1.9. Органы по аттестации аккредитуются Гостехкомиссией России. Правила аккредитации определяются действующим в системе "Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации".

Гостехкомиссия России может передавать права на аккредитацию отраслевых (ведомственных) органов по аттестации другим органам государственной власти.

1.10. Расходы по проведению всех видов работ и услуг по обязательной и добровольной аттестации объектов информатизации оплачивают заявители.

Оплата работ по обязательной аттестации производится в соответствии с договором по утвержденным расценкам, а при их отсутствии - по договорной цене в порядке, установленном Гостехкомиссией России по согласованию с Министерством финансов Российской Федерации.

Расходы по проведению всех видов работ и услуг по аттестации объектов информатизации оплачивают заявители за счет финансовых средств, выделенных на разработку (доработку) и введение в действие защищаемого объекта информатизации.

1.11. Органы по аттестации объектов информатизации несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонент.

2. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.

2.1. Организационную структуру системы аттестации объектов информатизации образуют:

- федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации - Гостехкомиссия России;

- органы по аттестации объектов информатизации по требованиям безопасности информации;

- испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;

- заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

2.2. Федеральный орган по сертификации и аттестации осуществляет следующие функции:

- организует обязательную аттестацию объектов информатизации;

- создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;

- устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;

- организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;

- аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;

- осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;

- рассматривает апелляции, возникающие в процессе аттестации объектов информатизации и контроля за эксплуатацией аттестованных объектов информатизации;

- организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

2.3. Органы по аттестации объектов информатизации аккредитуются Гостехкомиссией России и получают от нее лицензию на право проведения аттестации объектов информатизации.

Такими органами могут быть отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры Гостехкомиссии России.

2.4. Органы по аттестации:

- аттестуют объекты информатизации и выдают "Аттестаты соответствия";

- осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией;

- отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";

- формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;

- ведут информационную базу аттестованных этим органом объектов информатизации;

- осуществляют взаимодействие с Гостехкомиссией России и ежеквартально информируют его о своей деятельности в области аттестации.

2.5. Испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации по заказам заявителей проводят испытания несертифицированной продукции, используемой на объекте информатики, подлежащем обязательной аттестации, в соответствии с "Положением о сертификации средств защиты информации по требованиям безопасности информации".

2.6. Заявители:

- проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;

- привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;

- предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;

- привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;

- осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";

- извещают орган по аттестации, выдавший "Аттестат соответствия", о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");

- предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

3. Порядок проведения аттестации и контроля.

3.1. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

- подачу и рассмотрение заявки на аттестацию;

- предварительное ознакомление с аттестуемым объектом;

- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);

- разработка программы и методики аттестационных испытаний;

- заключение договоров на аттестацию;

- проведение аттестационных испытаний объекта информатизации;

- оформление, регистрация и выдача "Аттестата соответствия";

- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;

- рассмотрение апелляций.

3.2. Подача и рассмотрение заявки на аттестацию

3.2.1. Заявитель для получения "Аттестата соответствия" заблаговременно направляет в орган по аттестации заявку на проведение аттестации с исходными данными по аттестуемому объекту информатизации по форме, приведенной в приложении 1.

3.2.2. Орган по аттестации в месячный срок рассматривает заявку и на основании анализа исходных данных выбирает схему аттестации, согласовывает ее с заявителем и принимает решение о проведении аттестации объекта информатизации.

3.3. Предварительное ознакомление с аттестуемым объектом

При недостаточности исходных данных по аттестуемому объекту информатизации в схему аттестации включаются работы по предварительному ознакомлению с аттестуемым объектом, проводимые до этапа аттестационных испытаний.

3.4. Испытания несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте информатизации

3.4.1. При использовании на аттестуемом объекте информатизации несертифицированных средств и систем защиты информации в схему аттестации могут быть включены работы по их испытаниям в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации или непосредственно на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств.

3.4.2. Испытания отдельных несертифицированных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации проводятся до аттестационных испытаний объектов информатизации.

В этом случае заявителем к началу аттестационных испытаний должны быть представлены заключения органов по сертификации средств защиты информации по требованиям безопасности информации и сертификаты.

3.5. Разработка программы и методики аттестационных испытаний

3.5.1. По результатам рассмотрения заявки и анализа исходных данных, а также предварительного ознакомления с аттестуемым объектом органом по аттестации разрабатываются программа аттестационных испытаний, предусматривающая перечень работ и их продолжительность, методики испытаний (или используются типовые методики), определяются количественный и профессиональный состав аттестационной комиссии, назначаемой органом по аттестации объектов информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации или привлечения испытательных центров (лабораторий) по сертификации средств защиты информации по требованиям безопасности информации.

3.5.2. Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации.

3.5.3. Программа аттестационных испытаний согласовывается с заявителем.

3.6. Заключение договоров на аттестацию

3.6.1. Этап подготовки завершается заключением договора между заявителем и органом по аттестации на проведение аттестации, заключением договоров (контрактов) органа по аттестации с привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.

3.6.2. Оплата работы членов аттестационной комиссии производится органом по аттестации в соответствии с заключенными трудовыми договорами (контрактами) за счет финансовых средств от заключаемых договоров на аттестацию объектов информатизации.

3.7. Проведение аттестационных испытаний объектов информатизации

3.7.1. На этапе аттестационных испытаний объекта информатизации:

- осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;

- определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;

- проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;

- проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

- проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

- оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

3.7.2. Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи "Аттестата соответствия" и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя.

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протоколы испытаний подписываются экспертами - членами аттестационной комиссии, проводившими испытания.

Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

3.8. Оформление, регистрация и выдача "Аттестата соответствия"

3.8.1. "Аттестат соответствия" на объект информатизации, отвечающий требованиям по безопасности информации, выдается органом по аттестации по форме, приведенной в приложении 2.

3.8.2. "Аттестат соответствия" оформляется и выдается заявителю после утверждения заключения по результатам аттестации.

3.8.3. Регистрация "Аттестатов соответствия" осуществляется по отраслевому или территориальному признакам органами по аттестации с целью ведения информационной базы аттестованных объектов информатизации и планирования мероприятий по контролю и надзору.

Ведение сводных информационных баз аттестованных объектов информатизации осуществляется Гостехкомиссией России или по ее поручению одним из органов надзора за аттестацией и эксплуатацией аттестованных объектов.

3.8.4. "Аттестат соответствия" выдается владельцу аттестованного объекта информатизации органом по аттестации на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

3.8.5. В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации,

который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

3.8.6. При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки орган по аттестации принимает решение об отказе в выдаче "Аттестата соответствия".

При этом может быть предложен срок повторной аттестации при условии устранения недостатков.

При наличии замечаний непринципиального характера "Аттестат соответствия" может быть выдан после проверки устранения этих замечаний.

3.9. Рассмотрение апелляций

В случае несогласия заявителя с отказом в выдаче "Аттестата соответствия" он имеет право обратиться в вышестоящий орган по аттестации или непосредственно в Гостехкомиссию России с апелляцией для дополнительного рассмотрения полученных при испытаниях результатов, где она в месячный срок рассматривается с привлечением заинтересованных сторон. Податель апелляции извещается о принятом решении.

3.10. Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации

3.10.1. Государственный контроль и надзор, инспекционный контроль за проведением аттестации объектов информатизации проводится Гостехкомиссией России как в процессе, так и по завершении аттестации, а за эксплуатацией аттестованных объектов информатизации - периодически в соответствии с планами работы по контролю и надзору.

Гостехкомиссия России может передавать некоторые из своих функций государственного контроля и надзора по аттестации и за эксплуатацией аттестованных объектов информатизации аккредитованным органам по аттестации.

3.10.2. Объем, содержание и порядок государственного контроля и надзора устанавливаются в нормативной и методической документации по аттестации объектов информатизации.

3.10.3. Государственный контроль и надзор за соблюдением правил аттестации включает проверку правильности и полноты проводимых мероприятий по аттестации объектов информатизации, оформления и рассмотрения органами по аттестации отчетных документов и протоколов испытаний, своевременное внесение изменений в нормативную и методическую документацию по безопасности информации, инспекционный контроль за эксплуатацией аттестованных объектов информатизации.

3.10.4. В случае грубых нарушений органом по аттестации требований стандартов или иных нормативных и методических документов по безопасности информации, выявленных при контроле и надзоре, орган по аттестации может быть лишен лицензии на право проведения аттестации объектов информатизации.

3.10.5. При выявлении нарушения правил эксплуатации аттестованных объектов информатизации, технологии обработки защищаемой информации и требований по безопасности информации органом, проводящим контроль и надзор, может быть приостановлено или аннулировано действие "Аттестата соответствия", с оформлением

этого решения в "Аттестате соответствия" и информированием органа, ведущего сводную информационную базу аттестованных объектов информатики, и Гостехкомиссии России.

Решение об аннулировании действия "Аттестата соответствия" принимается в случае, когда в результате оперативного принятия организационно-технических мер защиты не может быть восстановлен требуемый уровень безопасности информации.

3.10.6. В случае грубых нарушений органом по аттестации требований стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России, выявленных при контроле и надзоре и приведших к повторной аттестации, расходы по осуществлению контроля и надзора могут быть по решению Госарбитража взысканы с органа по аттестации. Повторная аттестация может быть также осуществлена за счет этого органа по аттестации.

3.10.7. Расходы по осуществлению надзора за обязательной аттестацией и эксплуатацией объектов, прошедших обязательную аттестацию, оплачиваются органом надзора из средств госбюджета, выделенных ему в этих целях.

…….

1. 4 Лекция № 5 (2 часа).

Тема: «Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне"»

1.4.1 Вопросы лекции:

1. Общие положения.
2. Перечень сведений, составляющих государственную тайну.
3. Отнесение сведений к государственной тайне и их засекречивание.

…….

1.4.2 Краткое содержание вопросов:

1. Общие положения.

Статья 1. Сфера действия настоящего Закона

Положения настоящего Закона обязательны для исполнения на территории Российской Федерации и за ее пределами органами законодательной, исполнительной и судебной власти, а также организациями, наделенными в соответствии с федеральным законом полномочиями осуществлять от имени Российской Федерации государственное управление в установленной сфере деятельности (далее - органы государственной власти), органами местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.
(в ред. Федеральных законов от 06.10.1997 N 131-ФЗ, от 01.12.2007 N 318-ФЗ)

Статья 2. Основные понятия, используемые в настоящем Законе

В настоящем Законе используются следующие основные понятия:

государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

носители сведений, составляющих государственную тайну, - материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

система защиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;

доступ к сведениям, составляющим государственную тайну, - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Перечень сведений, составляющих государственную тайну, - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

(абзац введен Федеральным законом от 06.10.1997 N 131-ФЗ)

Статья 3. Законодательство Российской Федерации о государственной тайне

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации "О безопасности" и включает настоящий Закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

Статья 4. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты

1. Палаты Федерального Собрания:

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

осуществляют законодательное регулирование отношений в области государственной тайны;

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

абзац исключен. - Федеральный закон от 06.10.1997 N 131-ФЗ;

определяют полномочия должностных лиц в аппаратах палат Федерального Собрания по обеспечению защиты государственной тайны в палатах Федерального Собрания;

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

абзац исключен. - Федеральный закон от 06.10.1997 N 131-ФЗ.

2. Президент Российской Федерации:

утверждает государственные программы в области защиты государственной тайны;

утверждает по представлению Правительства Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;

утверждает по представлению Правительства Российской Федерации Перечень должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне, Перечень должностей, при замещении которых лица считаются допущенными к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;

(в ред. Федерального закона от 18.07.2009 N 180-ФЗ)

заключает международные договоры Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну;

определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента Российской Федерации;

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

3. Правительство Российской Федерации:

организует исполнение Закона Российской Федерации "О государственной тайне";

представляет на утверждение Президенту Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;

представляет на утверждение Президенту Российской Федерации Перечень должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне, Перечень должностей, при замещении которых лица считаются допущенными к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;

(в ред. Федерального закона от 18.07.2009 N 180-ФЗ)

устанавливает порядок разработки Перечня сведений, отнесенных к государственной тайне;

организует разработку и выполнение государственных программ в области защиты государственной тайны;

определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства Российской Федерации;

устанавливает порядок предоставления социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны, если социальные гарантии либо порядок предоставления таких социальных гарантий не установлены федеральными законами или нормативными правовыми актами Президента Российской Федерации;

(в ред. Федеральных законов от 22.08.2004 N 122-ФЗ, от 08.11.2011 N 309-ФЗ)

устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;

заключает межправительственные соглашения, принимает меры по выполнению международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам или международным организациям;

(в ред. Федерального закона от 01.12.2007 N 294-ФЗ)

в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

(абзац введен Федеральным законом от 06.10.1997 N 131-ФЗ)

4. Органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:

обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;

обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства Российской Федерации;

устанавливают размеры предоставляемых социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны на подведомственных им предприятиях, в учреждениях и организациях;

обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;

реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению социальных гарантий лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;

вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.

(п. 4 в ред. Федерального закона от 22.08.2004 N 122-ФЗ)

5. Органы судебной власти:

рассматривают уголовные, гражданские и административные дела о нарушениях законодательства Российской Федерации о государственной тайне;

(в ред. Федерального закона от 08.03.2015 N 23-ФЗ)

обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны;

обеспечивают в ходе рассмотрения указанных дел защиту государственной тайны;

определяют полномочия должностных лиц по обеспечению защиты государственной тайны в органах судебной власти.

2. Перечень сведений, составляющих государственную тайну.

Статья 5. Перечень сведений, составляющих государственную тайну

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Государственную тайну составляют:

1) сведения в военной области:

о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых

Российской Федерации (по списку, определяемому Правительством Российской Федерации);

(в ред. Федерального закона от 11.11.2003 N 153-ФЗ)

3) сведения в области внешней политики и экономики:

о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты:

(в ред. Федеральных законов от 15.11.2010 N 299-ФЗ, от 21.12.2013 N 377-ФЗ)

о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной, оперативно-розыскной деятельности и деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

(в ред. Федерального закона от 15.11.2010 N 299-ФЗ)

о силах, средствах, об источниках, о методах, планах и результатах деятельности по обеспечению безопасности лиц, в отношении которых принято решение о применении мер государственной защиты, данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения, а также отдельные сведения об указанных лицах;

(абзац введен Федеральным законом от 21.12.2013 N 377-ФЗ)

о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

о методах и средствах защиты секретной информации;

об организации и о фактическом состоянии защиты государственной тайны;

о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;

о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства;

о мерах по обеспечению защищенности критически важных объектов и потенциально опасных объектов инфраструктуры Российской Федерации от террористических актов;

(абзац введен Федеральным законом от 15.11.2010 N 299-ФЗ)

о результатах финансового мониторинга в отношении организаций и физических лиц, полученных в связи с проверкой их возможной причастности к террористической деятельности.

(абзац введен Федеральным законом от 15.11.2010 N 299-ФЗ)

3. Отнесение сведений к государственной тайне и их засекречивание.

Статья 6. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Отнесение сведений к государственной тайне и их засекречивание - введение в предусмотренном настоящим Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами законности, обоснованности и своевременности.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 настоящего Закона и законодательству Российской Федерации о государственной тайне.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Обоснованность отнесения сведений к государственной тайне и их засекречивание заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Своевременность отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Статья 7. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

(в ред. Федерального закона от 22.08.2004 N 122-ФЗ)

о фактах нарушения прав и свобод человека и гражданина;

о размерах золотого запаса и государственных валютных резервах Российской Федерации;

о состоянии здоровья высших должностных лиц Российской Федерации;

о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суд.

Статья 8. Степени секретности сведений и грифы секретности носителей этих сведений

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "особой важности", "совершенно секретно" и "секретно".

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Статья 9. Порядок отнесения сведений к государственной тайне

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с настоящим Законом.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым настоящим Законом, руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом Российской Федерации. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, Перечень сведений, отнесенных к государственной тайне. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом Российской Федерации, подлежит открытому опубликованию и пересматривается по мере необходимости.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые перечни сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности. В рамках целевых программ по разработке и модернизации образцов вооружения и военной техники, опытно-конструкторских и научно-исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться отдельные перечни сведений, подлежащих засекречиванию. Эти перечни утверждаются

соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.
(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Статья 10. Ограничение прав собственности предприятий, учреждений, организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием

Должностные лица, наделенные в порядке, предусмотренном статьей 9 настоящего Закона, полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан (далее - собственник информации), если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к государственной тайне. Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.

Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником. В договоре также предусматриваются обязательства собственника информации по ее нераспространению. При отказе собственника информации от подписанного договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну, в соответствии с действующим законодательством.

Собственник информации вправе обжаловать в суд действия должностных лиц, ущемляющие, по мнению собственника информации, его права. В случае признания судом действий должностных лиц незаконными порядок возмещения ущерба, нанесенного собственнику информации, определяется решением суда в соответствии с действующим законодательством.

Не может быть ограничено право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства Российской Федерации.

Статья 11. Порядок засекречивания сведений и их носителей

Основанием для засекречивания сведений, полученных (разработанных) в результате управленческой, производственной, научной и иных видов деятельности органов государственной власти, предприятий, учреждений и организаций, является их соответствие действующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию. При

засекречивании этих сведений их носителям присваивается соответствующий гриф секретности.

При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные лица органов государственной власти, предприятий, учреждений и организаций обязаны обеспечить предварительное засекречивание полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направить в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

Должностные лица, утвердившие действующий перечень, обязаны в течение трех месяцев организовать экспертную оценку поступивших предложений и принять решение по дополнению (изменению) действующего перечня или снятию предварительно присвоенного сведениям грифа секретности.

Статья 12. Реквизиты носителей сведений, составляющих государственную тайну

На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;

об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

о регистрационном номере;

о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, эти данные указываются в сопроводительной документации на этот носитель.

Если носитель содержит составные части с различными степенями секретности, каждой из этих составных частей присваивается соответствующий гриф секретности, а носителю в целом присваивается гриф секретности, соответствующий тому грифу секретности, который присваивается его составной части, имеющей высшую для данного носителя степень секретности сведений.

Помимо перечисленных в настоящей статье реквизитов на носителе и (или) в сопроводительной документации к нему могут проставляться дополнительные отметки, определяющие полномочия должностных лиц по ознакомлению с содержащимися в этом носителе сведениями. Вид и порядок проставления дополнительных отметок и других

реквизитов определяются нормативными документами, утверждаемыми Правительством Российской Федерации.

…….

1. 5 Лекция № 6 (2 часа).

Тема: «Организационно-технические меры защиты сведений, составляющих государственную тайну, обрабатываемых в автоматизированных информационных системах»

1.5.1 Вопросы лекции:

1. Организационно-технические меры защиты сведений, составляющих государственную тайну, обрабатываемых в автоматизированных информационных системах.

…….

1.5.2 Краткое содержание вопросов:

1. Организационно-технические меры защиты сведений, составляющих государственную тайну, обрабатываемых в автоматизированных информационных системах.

5.1.1. Система (подсистема) защиты информации, обрабатываемой в автоматизированных системах различного уровня и назначения, должна предусматривать комплекс организационных, программных, технических и, при необходимости, криптографических средств и мер по защите информации при ее автоматизированной обработке и хранении, при ее передаче по каналам связи.

5.1.2. Основными направлениями защиты информации являются:

обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения и подделки за счет НСД и специальных воздействий;

обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

5.1.3. В качестве основных мер защиты информации рекомендуются:

документальное оформление перечня сведений конфиденциального характера с учетом ведомственной и отраслевой специфики этих сведений;

реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам, документам;

ограничение доступа персонала и посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации;

разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

регистрация действий пользователей АС и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;

учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение;

использование СЗЗ, создаваемых на основе физико-химических технологий для контроля доступа к объектам защиты и для защиты документов от подделки;

необходимое резервирование технических средств и дублирование массивов и носителей информации;
использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;
использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;
использование сертифицированных средств защиты информации;
размещение объектов защиты на максимально возможном расстоянии относительно границы КЗ;
размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах КЗ;
развязка цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
электромагнитная развязка между линиями связи и другими цепями ВТСС, выходящими за пределы КЗ, и информационными цепями, по которым циркулирует защищаемая информация;
использование защищенных каналов связи (защищенных ВОЛС и криптографических средств ЗИ;
размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр информации;
организация физической защиты помещений и собственно технических средств с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающих нахождение внутри контролируемой зоны технических средств разведки или промышленного шпионажа;
криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи (при необходимости, определяемой особенностями функционирования конкретных АС и систем связи);
предотвращение внедрения в автоматизированные системы программ-вирусов, программных закладок.
Обязательность тех или иных мер для защиты различных видов конфиденциальной информации конкретизирована в последующих подразделах документа.
5.1.4. В целях дифференцированного подхода к защите информации, обрабатываемой в АС различного уровня и назначения, осуществляемого в целях разработки и применения необходимых и достаточных мер и средств защиты информации, проводится классификация автоматизированных систем (форма акта классификации АС приведена в приложении № 1).
5.1.5. Классифицируются АС любого уровня и назначения. Классификация АС осуществляется на основании требований РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" и настоящего раздела документа.
5.1.6. Классификации подлежат все действующие, но ранее не классифицированные, и разрабатываемые АС, предназначенные для обработки конфиденциальной информации.
5.1.7. Если АС, классифицированная ранее, включается в состав вычислительной сети или системы и соединяется с другими техническими средствами линиями связи различной физической природы, образуемая при этом АС более высокого уровня классифицируется в целом, а в отношении АС нижнего уровня классификация не производится.
Если объединяются АС различных классов защищенности, то интегрированная АС должна классифицироваться по высшему классу защищенности входящих в нее АС, за исключением случаев их объединения посредством межсетевого экрана, когда каждая из

объединяющихся АС может сохранять свой класс защищенности. Требования к используемым при этом межсетевым экранам изложены в подразделе 5.9.
5.1.8. При рассмотрении и определении режима обработки данных в АС учитывается, что индивидуальным (монопольным) режимом обработки считается режим, при котором ко всей обрабатываемой информации, к программным средствам и носителям информации этой системы допущен только один пользователь.
Режим, при котором различные пользователи, в т.ч. обслуживающий персонал и программисты, работают в одной АС, рассматривается как коллективный. Коллективным режимом работы считается также и последовательный во времени режим работы различных пользователей и обслуживающего персонала.
5.1.9. В случае, когда признаки классифицируемой АС (п. 1.7. РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации") не совпадают с предложенными в РД (п. 1.9) группами по особенностям обработки информации в АС, то при классификации выбирается наиболее близкая группа защищенности с предъявлением к АС соответствующих дополнительных требований по защите информации. (Например, однопользовательская АС с информацией различного уровня конфиденциальности по формальным признакам не может быть отнесена к 3 группе защищенности. Однако, если дополнительно реализовать в такой системе управление потоками информации, то необходимый уровень защиты будет обеспечен).
5.1.10. Конкретные требования по защите информации и мероприятия по их выполнению определяются в зависимости от установленного для АС класса защищенности. Рекомендуемые классы защищенности АС, СЗЗ, средств защиты информации по уровню контроля отсутствия недекларированных возможностей, а также показатели по классам защищенности СВТ и МЭ от несанкционированного доступа к информации приведены в приложении № 7.
5.1.11. Лица, допущенные к автоматизированной обработке конфиденциальной информации, несут ответственность за соблюдение ими установленного в учреждении (на предприятии) порядка обеспечения защиты этой информации.
Для получения доступа к конфиденциальной информации они должны изучить требования настоящего документа, других нормативных документов по защите информации, действующих в учреждении (на предприятии) в части их касающейся.

5.2. Основные требования и рекомендации по защите служебной тайны и персональных данных

При разработке и эксплуатации АС, предполагающих использование информации, составляющей служебную тайну, а также персональных данных должны выполняться следующие основные требования.
5.2.1. Организация, состав и содержание проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны отвечать требованиям раздела 3.
5.2.2. В учреждении (на предприятии) должны быть документально оформлены перечни сведений, составляющих служебную тайну, и персональных данных, подлежащих защите. Эти перечни могут носить как обобщающий характер в области деятельности учреждения (предприятия), так и иметь отношение к какому-либо отдельному направлению работ. Все исполнители должны быть ознакомлены с этими перечнями в части их касающейся.
5.2.3. В соответствии с РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" устанавливается следующий порядок классификации АС в зависимости от вида сведений конфиденциального характера:

АС, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г;
АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д.
5.2.4. Для обработки информации, составляющей служебную тайну, а также для обработки персональных данных следует использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).
Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.
5.2.5. Для передачи информации по каналам связи, выходящим за пределы КЗ, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации. Применяемые средства защиты информации должны быть сертифицированы.
5.2.6. Носители информации на магнитной (магнитно-оптической) и бумажной основе должны учитываться, храниться и уничтожаться в подразделениях учреждений (предприятий) в порядке, установленном для служебной информации ограниченного распространения, с пометкой "Для служебного пользования".
5.2.7. Доступ к информации исполнителей (пользователей, обслуживающего персонала) осуществляется в соответствии с разрешительной системой допуска исполнителей к документам и сведениям конфиденциального характера, действующей в учреждении (на предприятии).
5.2.8. При необходимости указанный минимальный набор рекомендуемых организационно-технических мер защиты информации по решению руководителя предприятия может быть расширен.

5.3. Основные рекомендации по защите информации, составляющей коммерческую тайну

При разработке и эксплуатации АС, предполагающих использование сведений, составляющих коммерческую тайну, рекомендуется выполнение следующих основных организационно-технических мероприятий:
5.3.1. На предприятии следует документально оформить "Перечень сведений, составляющих коммерческую тайну". Все исполнители должны быть ознакомлены с этим "Перечнем".
5.3.2. При организации разработки и эксплуатации АС с использованием таких сведений следует ориентироваться на порядок, приведенный в разделе 3. Оформить порядок разработки и эксплуатации таких АС документально.
5.3.3. Рекомендуется относить АС, обрабатывающие информацию, составляющую коммерческую тайну, режим защиты которой определяет ее собственник, по уровню защищенности к классам 3Б, 2Б и не ниже 1Д (если по решению руководителя предприятия не предъявляются более высокие требования).
5.3.4. Рекомендуется для обработки информации, составляющей коммерческую тайну, использовать средства вычислительной техники, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).
Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.

5.3.5. Для передачи информации по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации.
5.3.6. Следует установить на предприятии порядок учета, хранения и уничтожения носителей информации на магнитной (магнитно-оптической) и бумажной основе в научных, производственных и функциональных подразделениях, а также разработать и ввести в действие разрешительную систему допуска исполнителей документам и сведениям, составляющим коммерческую тайну.
Указанный минимальный набор рекомендуемых организационно-технических мероприятий по решению руководителя предприятия может быть расширен.
Решение о составе и содержании мероприятий, а также используемых средств защиты информации принимается руководителем предприятия по результатам обследования создаваемой (модернизируемой) АС с учетом важности (ценности) защищаемой информации.

5.4. Порядок обеспечения защиты конфиденциальной информации при эксплуатации АС

5.4.1. Организация эксплуатации АС и СЗИ в ее составе осуществляется в соответствии с установленным в учреждении (на предприятии) порядком, в том числе технологическими инструкциями по эксплуатации СЗИ НСД для пользователей, администраторов АС и работников службы безопасности.
5.4.2. Для обеспечения защиты информации в процессе эксплуатации АС рекомендуется предусматривать соблюдение следующих основных положений и требований:
допуск к защищаемой информации лиц, работающих в АС (пользователей, обслуживающего персонала), должен производиться в соответствии с установленным разрешительной системой допуска порядком;
на период обработки защищаемой информации в помещениях, где размещаются ОТСС, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации; допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в эти помещения только с санкции руководителя учреждения (предприятия) или руководителя службы безопасности;
в случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации;
по окончании обработки защищаемой информации или при передаче управления другому лицу пользователь обязан произвести стирание временных файлов на несъёмных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ПЭВМ;
изменение или ввод новых программ обработки защищаемой информации в АС должен осуществляться совместно разработчиком АС и администратором АС;
при увольнении или перемещении администраторов АС руководителем учреждения (предприятия) по согласованию со службой безопасности должны быть приняты меры по оперативному изменению паролей, идентификаторов и ключей шифрования.
5.4.3. Все носители информации на бумажной, магнитной, оптической (магнито-оптической) основе, используемые в технологическом процессе обработки информации в АС, подлежат учету в том производственном, научном или функциональном подразделении, которое является владельцем АС, обрабатывающей эту информацию.
5.4.4. Учет съемных носителей информации на магнитной или оптической основе (гибкие магнитные диски, съемные накопители информации большой емкости или картриджи, съемные пакеты дисков, иные магнитные, оптические или магнито-оптические диски, магнитные ленты и т.п.), а также распечаток текстовой, графической и иной информации

на бумажной или пластиковой (прозрачной) основе осуществляется по карточкам или журналам установленной формы, в том числе автоматизировано с использованием средств вычислительной техники. Журнальная форма учета может использоваться в АС с небольшим объемом документооборота.
5.4.5. Съемные носители информации на магнитной или оптической основе в зависимости от характера или длительности использования допускается учитывать совместно с другими документами по установленным для этого учетным формам.
При этом перед выполнением работ сотрудником, ответственным за их учет, на этих носителях информации предварительно проставляются любым доступным способом следующие учетные реквизиты: учетный номер и дата, пометка "Для служебного пользования", номер экземпляра, подпись этого сотрудника, а также другие возможные реквизиты, идентифицирующие этот носитель.
5.4.6. Распечатки допускается учитывать совместно с другими традиционными печатными документами по установленным для этого учетным формам.
5.4.7. Временно не используемые носители информации должны храниться пользователем в местах, недоступных для посторонних лиц.

5.5. Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ

5.5.1. Автоматизированные рабочие места на базе автономных ПЭВМ являются автоматизированными системами, обладающими всеми основными признаками АС. Информационным каналом обмена между такими АС являются носители информации на магнитной (магнитно-оптической) и бумажной основе.
В связи с этим порядок разработки и эксплуатации АРМ на базе автономных ПЭВМ по составу и содержанию проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны полностью отвечать требованиям настоящего документа.
5.5.2. АС на базе автономных ПЭВМ в соответствии с требованиями РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" должны быть классифицированы и отнесены:
к 3 группе АС, если в ней работает только один пользователь, допущенный ко всей информации АС;
ко 2 и 1 группе АС, если в ней последовательно работают несколько пользователей с равными или разными правами доступа (полномочиями), соответственно.
Примечание: При использовании на автономной ПЭВМ технологии обработки информации на съемных накопителях большой емкости, классификация АС производится на основании анализа режима доступа пользователей АС к информации на используемом съемном накопителе (либо одновременно используемом их комплексе).

5.6. Защита информации при использовании съемных накопителей информации большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ

5.6.1. Данная информационная технология предусматривает запись на загружаемый съемный накопитель информации большой емкости одновременно общесистемного (ОС, СУБД) и прикладного программного обеспечения, а также обрабатываемой информации одного или группы пользователей.
В качестве устройств для работы по этой технологии могут быть использованы накопители на магнитном, магнито-оптическом или лазерном дисках различной конструкции, как встроенные (съемные), так и выносные. Одновременно может быть установлено несколько съемных накопителей информации большой емкости.
Несъемные накопители должны быть исключены из конфигурации ПЭВМ.

Основной особенностью применения данной информационной технологии для АРМ на базе автономных ПЭВМ с точки зрения защиты информации является исключение этапа хранения на ПЭВМ в нерабочее время информации, подлежащей защите.
Эта особенность может быть использована для обработки защищаемой информации без применения сертифицированных средств защиты информации от НСД и использования средств физической защиты помещений этих АРМ.
5.6.2. На этапе предпроектного обследования необходимо провести детальный анализ технологического процесса обработки информации, обращая внимание, прежде всего, на технологию обмена информацией (при использовании съемных накопителей информации большой емкости или гибких магнитных дисков (ГМД или дискет) с другими АРМ, как использующими, так и не использующими эту информационную технологию, на создание условий, исключающих попадание конфиденциальной информации на неучтенные носители информации, несанкционированное ознакомление с этой информацией, на организацию выдачи информации на печать.
5.6.3. Обмен конфиденциальной информацией между АРМ должен осуществляться только на учтенных носителях информации с учетом допуска исполнителей, работающих на АРМ, к переносимой информации.
5.6.4. На рабочих местах исполнителей, работающих по этой технологии, во время работы, как правило, не должно быть неучтенных накопителей информации.
В случае формирования конфиденциальных документов с использованием, как текстовой, так и графической информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть "закрыты на запись".
Условия и порядок применения таких процедур должны быть отражены в технологии обработки информации, использующей съемные накопители информации большой емкости.
5.6.5. При использовании в этой технологии современных средств вычислительной техники, оснащенных энергонезависимой, управляемой извне перезаписываемой памятью, так называемых Flash-Bios (FB), необходимо обеспечить целостность записанной в FB информации. Для обеспечения целостности, как перед началом работ, с конфиденциальной информацией при загрузке ПЭВМ, так и по их окончании, необходимо выполнить процедуру проверки целостности FB. При несовпадении необходимо восстановить (записать первоначальную версию) FB, поставить об этом в известность руководителя подразделения и службу безопасности, а также выяснить причины изменения FB.
5.6.6. Должна быть разработана и по согласованию с службой безопасности утверждена руководителем учреждения (предприятия) технология обработки конфиденциальной информации, использующая съемные накопители информации большой емкости и предусматривающая вышеуказанные, а также другие вопросы защиты информации, имеющие отношение к условиям размещения, эксплуатации АРМ, учету носителей информации, а также другие требования, вытекающие из особенностей функционирования АРМ.

5.7. Защита информации в локальных вычислительных сетях

5.7.1. Характерными особенностями ЛВС являются распределенное хранение файлов, удаленная обработка данных (вычисления) и передача сообщений (электронная почта), а также сложность проведения контроля за работой пользователей и состоянием общей безопасности ЛВС.
5.7.2. Средства защиты информации от НСД должны использоваться во всех узлах ЛВС независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС и требуют постоянного квалифицированного сопровождения со стороны администратора безопасности информации.

5.7.3. Информация, составляющая служебную тайну, и персональные данные могут обрабатываться только в изолированных ЛВС, расположенных в пределах контролируемой зоны, или в условиях, изложенных в пунктах 5.8.4. и 5.8.5. следующего подраздела.
5.7.4. Класс защищенности ЛВС определяется в соответствии с требованиями РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации".
5.7.5. Для управления ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, в дополнение к системным администраторам (администраторам ЛВС) могут быть назначены администраторы по безопасности информации, имеющие необходимые привилегии доступа к защищаемой информации ЛВС.
5.7.6. Состав пользователей ЛВС должен устанавливаться по письменному разрешению руководства предприятия (структурного подразделения) и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.
5.7.7. Каждый администратор и пользователь должен иметь уникальные идентификаторы и пароли, а в случае использования криптографических средств защиты информации - ключи шифрования для криптографических средств, используемых для защиты информации при передаче ее по каналам связи и хранения, и для систем электронной цифровой подписи.

5.8. Защита информации при межсетевом взаимодействии

5.8.1. Положения данного подраздела относятся к взаимодействию локальных сетей, ни одна из которых не имеет выхода в сети общего пользования типа Internet.
5.8.2. Взаимодействие ЛВС с другими вычислительными сетями должно контролироваться с точки зрения защиты информации. Коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах КЗ.
5.8.3. При конфигурировании коммуникационного оборудования (маршрутизаторов, концентраторов, мостов и мультиплексоров) и прокладке кабельной системы ЛВС рекомендуется учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия.
5.8.4. Подключение ЛВС к другой автоматизированной системе (локальной или неоднородной вычислительной сети) иного класса защищенности должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".
5.8.5. Для защиты конфиденциальной информации при ее передаче по каналам связи из одной АС в другую необходимо использовать:
в АС класса 1Г - МЭ не ниже класса 4;
в АС класса 1Д и 2Б, 3Б - МЭ класса 5 или выше.
Если каналы связи выходят за пределы КЗ, необходимо использовать защищенные каналы связи, защищенные волоконно-оптические линии связи либо сертифицированные криптографические средства защиты.

5.9. Защита информации при работе с системами управления базами данных

5.9.1. При работе с системами управления базами данных (СУБД) и базами данных (БД) необходимо учитывать следующие особенности защиты информации от НСД:
в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;

БД могут быть физически распределены по различным устройствам и узлам сети;
БД могут включать информацию различного уровня конфиденциальности;
разграничение доступа пользователей к БД средствами операционной системы и/или СЗИ НСД может осуществляться только на уровне файлов БД;
разграничение доступа пользователей к объектам БД: таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п., может осуществляться только средствами СУБД, если таковые имеются;
регистрация действий пользователей при работе с объектами БД может осуществляться также только средствами СУБД, если таковые имеются;
СУБД могут обеспечивать одновременный доступ многих пользователей (клиентов) к БД с помощью сетевых протоколов, при этом запросы пользователя к БД обрабатываются на сервере и результаты обработки направляются пользователям (клиентам).
5.9.2. С учетом указанных особенностей при создании БД рекомендуется:
при выборе СУБД ориентироваться на операционные системы и СУБД, включающие либо штатные сертифицированные средства защиты информации от НСД, либо имеющие соответствующие сертифицированные дополнения в виде СЗИ НСД;
при использовании СУБД, не имеющих средств разграничения доступа, производить разбиение БД на отдельные файлы, разграничение доступа к которым можно проводить средствами ОС и/или СЗИ НСД;
при использовании современных СУБД, основанных на модели клиент-сервер, использовать их штатные средства защиты информации от НСД, применять средства регистрации (аудита) и разграничение доступа к объектам БД на основе прав, привилегий, ролей, представлений (VIEW), процедур и т.п.

…….

1. 6 Лекция № 7 (2 часа).

Тема: «Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации»

1.6.1 Вопросы лекции:

1. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.
2. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации.
3. Государственное регулирование в сфере применения информационных технологий.

……

1.6.2 Краткое содержание вопросов:

1. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

2. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Статья 5. Информация как объект правовых отношений

1. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения

доступа к информации либо иные требования к порядку ее предоставления или распространения.

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Статья 6. Обладатель информации

1. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

3. Государственное регулирование в сфере применения информационных технологий.

Статья 12. Государственное регулирование в сфере применения информационных технологий

1. Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей;

4) обеспечение информационной безопасности детей.

(п. 4 введен Федеральным законом от 21.07.2011 N 252-ФЗ)

2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Статья 12.1. Особенности государственного регулирования в сфере использования российских программ для электронных вычислительных машин и баз данных

(введена Федеральным законом от 29.06.2015 N 188-ФЗ)

1. В целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки создается единый реестр российских программ для электронных вычислительных машин и баз данных (далее - реестр российского программного обеспечения).

2. Правила формирования и ведения реестра российского программного обеспечения, состав сведений, включаемых в реестр российского программного обеспечения, в том числе об основаниях возникновения исключительного права у правообладателя (правообладателей), условия включения таких сведений в реестр российского программного обеспечения и исключения их из реестра российского программного обеспечения, порядок предоставления сведений, включаемых в реестр российского программного обеспечения, порядок принятия решения о включении таких сведений в реестр российского программного обеспечения устанавливаются Правительством Российской Федерации.

3. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра российского программного обеспечения оператора реестра российского программного обеспечения - организацию, зарегистрированную на территории Российской Федерации.

4. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти утверждает классификатор программ для электронных вычислительных машин и баз данных в целях ведения реестра российского программного обеспечения.

5. В реестр российского программного обеспечения включаются сведения о программах для электронных вычислительных машин и базах данных, которые соответствуют следующим требованиям:

1) исключительное право на программу для электронных вычислительных машин или базу данных на территории всего мира и на весь срок действия исключительного права принадлежит одному либо нескольким из следующих лиц (правообладателей):

а) Российской Федерации, субъекту Российской Федерации, муниципальному образованию;

б) российской некоммерческой организации, высший орган управления которой формируется прямо и (или) косвенно Российской Федерацией, субъектами Российской Федерации, муниципальными образованиями и (или) гражданами Российской Федерации и решения которой иностранное лицо не имеет возможности определять в силу особенностей отношений между таким иностранным лицом и российской некоммерческой организацией;

в) российской коммерческой организации, в которой суммарная доля прямого и (или) косвенного участия Российской Федерации, субъектов Российской Федерации, муниципальных образований, российских некоммерческих организаций, указанных в подпункте "б" настоящего пункта, граждан Российской Федерации составляет более пятидесяти процентов;

г) гражданину Российской Федерации;

2) программа для электронных вычислительных машин или база данных правомерно введена в гражданский оборот на территории Российской Федерации, экземпляры программы для электронных вычислительных машин или базы данных либо права использования программы для электронных вычислительных машин или базы данных свободно реализуются на всей территории Российской Федерации;

3) общая сумма выплат по лицензионным и иным договорам, предусматривающим предоставление прав на результаты интеллектуальной деятельности и средства индивидуализации, выполнение работ, оказание услуг в связи с разработкой, адаптацией и модификацией программы для электронных вычислительных машин или базы данных и для разработки, адаптации и модификации программы для электронных вычислительных машин или базы данных, в пользу иностранных юридических лиц и (или) физических лиц, контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций, агентов, представителей иностранных лиц и контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций составляет менее тридцати процентов от выручки правообладателя (правообладателей) программы для электронных вычислительных машин или базы данных от реализации программы для электронных вычислительных машин или базы данных, включая предоставление прав использования, независимо от вида договора за календарный год;

4) сведения о программе для электронных вычислительных машин или базе данных не составляют государственную тайну, и программа для электронных вычислительных машин или база данных не содержит сведений, составляющих государственную тайну.

6. Правительством Российской Федерации могут быть установлены дополнительные требования к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения.

7. Программы для электронных вычислительных машин и базы данных, сведения о которых включены в реестр российского программного обеспечения, признаются происходящими из Российской Федерации.

8. Для целей настоящей статьи доля участия одной организации в другой организации или гражданина Российской Федерации в организации определяется в соответствии с порядком, установленным главой 14.1 Налогового кодекса Российской Федерации.

9. Для целей настоящей статьи контролируемой иностранным лицом российской коммерческой организацией или российской некоммерческой организацией признается организация, решения которой иностранное лицо имеет возможность определять в силу преобладающего прямого и (или) косвенного участия в этой организации, участия в договоре (соглашении), предметом которого является управление этой организацией, или иных особенностей отношений между иностранным лицом и этой организацией и (или) иными лицами.

10. Решение об отказе во включении в реестр российского программного обеспечения программ для электронных вычислительных машин или баз данных может быть обжаловано правообладателем программы для электронных вычислительных машин или базы данных в суд в течение трех месяцев со дня получения такого решения.

…….

1. 7 Лекция № 8 (2 часа).

Тема: «Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"»

1.7.1 Вопросы лекции:

1. Законодательство Российской Федерации о коммерческой тайне.
2. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации.
3. Охрана конфиденциальности информации.

…….

1.7.2 Краткое содержание вопросов:

1. Законодательство Российской Федерации о коммерческой тайне.

Статья 1. Цели и сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

(часть 1 в ред. Федерального закона от 12.03.2014 N 35-ФЗ)

2. Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

3. Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Статья 2. Утратила силу с 1 октября 2014 года. - Федеральный закон от 12.03.2014 N 35-ФЗ.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы,

избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;
(п. 1 в ред. Федерального закона от 18.12.2006 N 231-ФЗ)

2) информация, составляющая коммерческую тайну, - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;
(п. 2 в ред. Федерального закона от 12.03.2014 N 35-ФЗ)

3) утратил силу с 1 января 2008 года. - Федеральный закон от 18.12.2006 N 231-ФЗ;

4) обладатель информации, составляющей коммерческую тайну, - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

5) доступ к информации, составляющей коммерческую тайну, - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

6) передача информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

7) контрагент - сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

8) предоставление информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

9) разглашение информации, составляющей коммерческую тайну, - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Статья 4. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации

1. Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.

2. Утратил силу с 1 января 2008 года. - Федеральный закон от 18.12.2006 N 231-ФЗ.

3. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

4. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

2. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации.

Статья 4. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации

1. Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.

2. Утратил силу с 1 января 2008 года. - Федеральный закон от 18.12.2006 N 231-ФЗ.

3. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

4. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

Статья 5. Сведения, которые не могут составлять коммерческую тайну

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

3. Охрана конфиденциальности информации.

Статья 10. Охрана конфиденциальности информации

1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

(п. 5 в ред. Федерального закона от 11.07.2011 N 200-ФЗ)

2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.

3. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране конфиденциальности информации, указанные в части 1 настоящей статьи, за исключением пунктов 1 и 2, а также положений пункта 4, касающихся регулирования трудовых отношений.

4. Наряду с мерами, указанными в части 1 настоящей статьи, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Статья 11. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений

(в ред. Федерального закона от 12.03.2014 N 35-ФЗ)

1. В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан:

1) ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

2. Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

3. В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работник обязан:

1) выполнять установленный работодателем режим коммерческой тайны;

2) не разглашать эту информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

3) возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

4) передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну.

4. Работодатель вправе потребовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если эта информация разглашена в течение срока действия режима коммерческой тайны.

5. Причиненные работником или прекратившим трудовые отношения с работодателем лицом убытки не возмещаются, если разглашение информации, составляющей коммерческую тайну, произошло вследствие несоблюдения работодателем мер по обеспечению режима коммерческой тайны, действий третьих лиц или непреодолимой силы.

6. Трудовым договором с руководителем организации должны предусматриваться его обязанности по обеспечению охраны конфиденциальности составляющей коммерческую тайну информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны конфиденциальности этой информации.

7. Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством.

8. Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

…….

1. 8 Лекция № 9 (2 часа).

Тема: «Организационно-технические меры защиты коммерческой тайны, обрабатываемой в автоматизированных информационных системах»

1.8.1 Вопросы лекции:

1. Организационно-технические меры защиты коммерческой тайны, обрабатываемой в автоматизированных информационных системах.

…….

1.8.2 Краткое содержание вопросов:

1. Организационно-технические меры защиты коммерческой тайны, обрабатываемой в автоматизированных информационных системах.

2.1. Настоящий документ устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты конфиденциальной информации на территории Российской Федерации и является основным руководящим документом в этой области для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, предприятий, учреждений и организаций (далее - учреждения и предприятия) независимо от их организационно-правовой формы и формы собственности, должностных лиц и граждан Российской Федерации, взявшим на себя обязательства либо обязанными по статусу исполнять требования правовых документов Российской Федерации по защите информации.

2.2. Требования и рекомендации настоящего документа распространяются на защиту:

- конфиденциальной информации - информации с ограниченным доступом, за исключением сведений, отнесенных к государственной тайне и персональным данным, содержащейся в государственных (муниципальных) информационных ресурсах, накопленной за счет государственного (муниципального) бюджета и являющейся собственностью государства (к ней может быть отнесена информация, составляющая служебную тайну и другие виды тайн в соответствии с законодательством Российской Федерации, а также сведения конфиденциального характера в соответствии с "Перечнем сведений конфиденциального характера", утвержденного Указом Президента Российской Федерации от 06.03.97 №188), защита которой осуществляется в интересах государства (далее - служебная тайна);
- информации о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющей идентифицировать его личность (персональные данные) *(В соответствии с Федеральным законом "Об информации, информатизации и защите информации" режим защиты персональных данных должен быть определен федеральным законом. До его введения в действие для установления режима защиты*

такой информации следует руководствоваться настоящим документом., за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.)

2.3. Для защиты конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой определяет собственник этих ресурсов (например, информации, составляющей коммерческую, банковскую тайну и т.д.) (далее - коммерческая тайна), данный документ носит рекомендательный характер.

2.4. Документ разработан на основании федеральных законов "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", Указа Президента Российской Федерации от 06.03.97г. № 188 "Перечень сведений конфиденциального характера", "Доктрины информационной безопасности Российской Федерации", утвержденной Президентом Российской Федерации 09.09.2000г. № Пр.-1895, "Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти", утвержденного постановлением Правительства Российской Федерации от 03.11.94г. № 1233, других нормативных правовых актов по защите информации (приложение № 8), а также опыта реализации мер защиты информации в министерствах и ведомствах, в учреждениях и на предприятиях.

2.5. Документ определяет следующие основные вопросы защиты информации:

- организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;
- состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;
- требования и рекомендации по защите речевой информации при осуществлении переговоров, в том числе с использованием технических средств;
- требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;
- порядок обеспечения защиты информации при эксплуатации объектов информатизации;
- особенности защиты информации при разработке и эксплуатации автоматизированных систем, использующих различные типы средств вычислительной техники и информационные технологии;
- порядок обеспечения защиты информации при взаимодействии абонентов с информационными сетями общего пользования.

Порядок разработки, производства, реализации и использования средств криптографической защиты информации определяется "Положением о порядке разработки, производства (изготовления), реализации, приобретения и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну" (Положение ПКЗ-99), а также "Инструкцией по организации и обеспечению безопасности хранения, обработки и передачи по техническим каналам связи конфиденциальной информации в Российской Федерации с использованием сертифицированных ФАПСИ криптографических средств".

2.6. Защита информации, обрабатываемой с использованием технических средств, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в установленном настоящим документом порядке в виде системы (подсистемы) защиты информации во взаимосвязи с другими мерами по защите информации.

2.7. Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных электрических

сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в АС.

Защищаемыми объектами информатизации являются:

- средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации;
- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);
- защищаемые помещения.

2.8. Защита информации должна осуществляться посредством выполнения комплекса мероприятий и применение (при необходимости) средств ЗИ по предотвращению утечки информации или воздействия на нее по техническим каналам, за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

2.9. При ведении переговоров и использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

- акустическое излучение информативного речевого сигнала;
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы КЗ;
- виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
- несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;
- воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;
- побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;
- наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;
- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;

- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом;
- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- прослушивание ведущихся телефонных и радиопереговоров;
- просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

2.10. Перехват информации или воздействие на нее с использованием технических средств могут вестись:

- из-за границы КЗ из близлежащих строений и транспортных средств;
- из смежных помещений, принадлежащих другим учреждениям (предприятиям) и расположенным в том же здании, что и объект защиты;
- при посещении учреждения (предприятия) посторонними лицами;
- за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через информационные сети общего пользования.

2.11. В качестве аппаратуры перехвата или воздействия на информацию и технические средства могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта защиты либо подключаемые к каналам связи или техническим средствам обработки информации, а также электронные устройства перехвата информации "закладки", размещаемые внутри или вне защищаемых помещений.

2.12. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

- непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;
- случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;
- некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;
- просмотра информации с экранов дисплеев и других средств ее отображения.

2.13. Выявление и учет факторов воздействующих или могущих воздействовать на защищаемую информацию (угроз безопасности информации) в конкретных условиях, в соответствии с ГОСТ Р 51275-99, составляют основу для планирования и осуществления мероприятий, направленных на защиту информации на объекте информатизации.

Перечень необходимых мер защиты информации определяется по результатам обследования объекта информатизации с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения санкционированной доступности информации и работоспособности технических средств, обрабатывающих эту информацию, а также с учетом реальных возможностей ее перехвата и раскрытия ее содержания.

2.14. Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности информации реализуются без применения сложных технических средств перехвата информации:

- речевой информации, циркулирующей в защищаемых помещениях;
- информации, обрабатываемой средствами вычислительной техники, от несанкционированного доступа и несанкционированных действий;
- информации, выводимой на экраны видеомониторов;
- информации, передаваемой по каналам связи, выходящим за пределы КЗ.

2.15. Разработка мер и обеспечение защиты информации осуществляются подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководством предприятия (учреждения) для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии Гостехкомиссии России и/или ФАПСИ на право оказания услуг в области защиты информации.

2.16. Для защиты информации рекомендуется использовать сертифицированные по требованиям безопасности информации технические средства обработки и передачи информации, технические и программные средства защиты информации.

При обработке документированной конфиденциальной информации на объектах информатизации в органах государственной власти Российской Федерации и органах государственной власти субъектов Российской Федерации, других государственных органах, предприятиях и учреждениях средства защиты информационных систем подлежат обязательной сертификации.

2.17. Объекты информатизации должны быть аттестованы на соответствие требованиям по защите информации *(Здесь и далее под аттестацией понимается комиссионная приемка объекта информатизации силами предприятия с обязательным участием специалиста по защите информации.)*

2.18. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителей учреждений и предприятий, эксплуатирующих объекты информатизации.

…….

1. 9 Лекция № 10 (2 часа).

Тема: «Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

1.9.1 Вопросы лекции:

1. Общие положения.
2. Требования к организации защиты информации, содержащейся в информационной системе.
3. Формирование требований к защите информации, содержащейся в информационной системе.

…….

1.9.2 Краткое содержание вопросов:

1. Общие положения.

1. Настоящие Требования разработаны в соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328), а также с

учетом национальных стандартов Российской Федерации в области защиты информации и в области создания автоматизированных систем (далее – национальные стандарты).

2. В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее – защита информации) при обработке указанной информации в государственных информационных системах.

Настоящие Требования могут применяться для защиты общедоступной информации, содержащейся в государственных информационных системах, для достижения целей, указанных в пунктах 1 и 3 части 1 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации». В документе не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

3. Настоящие Требования являются обязательными при обработке информации в государственных информационных системах, функционирующих на территории Российской Федерации, а также в муниципальных информационных системах, если иное не установлено законодательством Российской Федерации о местном самоуправлении.

Настоящие Требования не распространяются на государственные информационные системы Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, Высшего Арбитражного Суда Российской Федерации и Федеральной службы безопасности Российской Федерации.

4. Настоящие Требования предназначены для обладателей информации, заказчиков, заключивших государственный контракт на создание государственной информационной системы (далее – заказчики) и операторов государственных информационных систем (далее – операторы).

Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (далее – уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии с настоящими Требованиями.

5. При обработке в государственной информационной системе информации, содержащей персональные данные, настоящие Требования применяются наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

6. По решению обладателя информации (заказчика) или оператора настоящие Требования могут применяться для защиты информации, содержащейся в негосударственных информационных системах.

7. Защита информации, содержащейся в государственной информационной системе (далее – информационная система), обеспечивается путем выполнения обладателем информации (заказчиком) и (или) оператором требований к организации защиты информации, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе.

2. Требования к организации защиты информации, содержащейся в информационной системе.

8. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

9. Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

10. Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности» (Собрание законодательства Российской Федерации, 2011, N 19, ст. 2716; N 30, ст. 4590; N 43, ст. 5971; N 48, ст. 6728; 2012, N 26, ст. 3446; N 31, ст. 4322; 2013, N 9, ст. 874).

11. Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании» (Собрание законодательства Российской Федерации, 2002, N 52, ст. 5140; 2007, N 19, ст. 2293; N 49, ст. 6070; 2008, N 30, ст. 3616; 2009, N 29, ст. 3626; N 48, ст. 5711; 2010, N 1, ст. 6; 2011, N 30, ст. 4603; N 49, ст. 7025; N 50, ст. 7351; 2012, N 31, ст. 4322; 2012, N 50, ст. 6959).

12. Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее – система защиты информации информационной системы).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

неправомерного блокирования информации (обеспечение доступности информации).

13. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

разработка системы защиты информации информационной системы;

внедрение системы защиты информации информационной системы;

аттестация информационной системы по требованиям защиты информации (далее –

аттестация информационной системы) и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

3. Формирование требований к защите информации, содержащейся в информационной системе.

14. Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации (заказчиком).

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее - ГОСТ Р 51583) и ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее - ГОСТ Р 51624) и в том числе включает:

принятие решения о необходимости защиты информации, содержащейся в информационной системе;

классификацию информационной системы по требованиям защиты информации (далее – классификация информационной системы);

определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

определение требований к системе защиты информации информационной системы.

14.1. При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:

анализ целей создания информационной системы и задач, решаемых этой информационной системой;

определение информации, подлежащей обработке в информационной системе;

анализ нормативных правовых актов, методических документов и национальных стандартов,

которым должна соответствовать информационная система;

принятие решения о необходимости создания системы защиты информации информационной системы, а также определение целей и задач защиты информации в информационной системе, основных этапов создания системы защиты информации информационной системы и функций по обеспечению защиты информации, содержащейся в информационной системе, обладателя информации (заказчика), оператора и уполномоченных лиц.

14.2. Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый).

Устанавливаются четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый. Класс защищенности информационной системы определяется в соответствии с приложением N 1 к настоящим Требованиям.

Класс защищенности определяется для информационной системы в целом и, при необходимости, для ее отдельных сегментов (составных частей). Требование к классу защищенности включается в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (далее – ГОСТ 34.602), ГОСТ Р 51583 и ГОСТ Р 51624.
Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Результаты классификации информационной системы оформляются актом классификации.

14.3. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации

угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818).

14.4. Требования к системе защиты информации информационной системы определяются в зависимости от класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации. Требования к системе защиты информации информационной системы включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

цель и задачи обеспечения защиты информации в информационной системе;

класс защищенности информационной системы;

перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

перечень объектов защиты информационной системы;

требования к мерам и средствам защиты информации, применяемым в информационной системе;

требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

При определении требований к системе защиты информации информационной системы учитываются положения политик обеспечения информационной безопасности обладателя информации (заказчика) в случае их разработки по ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», а также политик обеспечения информационной безопасности оператора и уполномоченного лица в части, не противоречащей политикам обладателя информации (заказчика).

…….

1. 10 Лекция № 11 (2 часа).

Тема: «Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.12.2013) "О персональных данных"»

1.10.1 Вопросы лекции:

1. Сфера действия настоящего Федерального закона.
2. Принципы и условия обработки персональных данных.
3. Право субъекта персональных данных на доступ к его персональным данным.

……

1.10.2 Краткое содержание вопросов:

1. Сфера действия настоящего Федерального закона.

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

(часть 1 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) утратил силу. - Федеральный закон от 25.07.2011 N 261-ФЗ;

4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

5) предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации".

(п. 5 введен Федеральным законом от 28.06.2010 N 123-ФЗ)

Статья 2. Цель настоящего Федерального закона

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

В целях настоящего Федерального закона используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Принципы и условия обработки персональных данных.

Статья 5. Принципы обработки персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Статья 6. Условия обработки персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
(в ред. Федерального закона от 05.04.2013 N 43-ФЗ)

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
(п. 5 в ред. Федерального закона от 21.12.2013 N 363-ФЗ)

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности

при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Статья 7. Конфиденциальность персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Статья 8. Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.
(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.
(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Статья 9. Согласие субъекта персональных данных на обработку его персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство

наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона, возлагается на оператора.

КонсультантПлюс: примечание.
В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 02.07.2013) в случаях, если федеральными законами и иными нормативными правовыми актами, вступившими в силу до 1 июля 2013 года, предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись.

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

Статья 10. Специальные категории персональных данных

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные сделаны общедоступными субъектом персональных данных;

(п. 2 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

(п. 2.1 введен Федеральным законом от 25.11.2009 N 266-ФЗ)

2.2) обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";

(п. 2.2 введен Федеральным законом от 27.07.2010 N 204-ФЗ)

2.3) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

(п. 2.3 введен Федеральным законом от 25.07.2011 N 261-ФЗ, в ред. Федерального закона от 21.07.2014 N 216-ФЗ)

3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

(п. 3 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-

социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

(п. 6 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

(п. 7 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

7.1) обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

(п. 7.1 введен Федеральным законом от 23.07.2013 N 205-ФЗ)

8) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

(п. 8 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

9) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;

(п. 9 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

10) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

(п. 10 введен Федеральным законом от 04.06.2014 N 142-ФЗ)

3. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

4. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных частями 2 и 3 настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.
(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Статья 11. Биометрические персональные данные

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.
(в ред. Федерального закона от 04.06.2014 N 142-ФЗ)

Статья 12. Трансграничная передача персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Статья 13. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных

1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей

государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

3. Право субъекта персональных данных на доступ к его персональным данным.

Статья 14. Право субъекта персональных данных на доступ к его персональным данным

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения, указанные в части 7 настоящей статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

КонсультантПлюс: примечание.
В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 02.07.2013) в случаях, если федеральными законами и иными нормативными правовыми актами, вступившими в силу до 1 июля 2013 года, предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись.

3. Сведения, указанные в части 7 настоящей статьи, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. В случае, если сведения, указанные в части 7 настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 настоящей статьи, должен содержать обоснование направления повторного запроса.

6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

…….

1. 11 Лекция № 12 (2 часа).

Тема: «Требования к защите персональных данных при их обработке в информационных системах персональных данных»

1.11.1 Вопросы лекции:

1. Общие положения.
2. Типы угроз безопасности персональных данных.
3. Уровни защищенности персональных данных.

…….

1.11.2 Краткое содержание вопросов:

1. Общие положения.

1. Настоящий документ разработан в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; 2011, N 23, ст. 3263; N 31, ст. 4701) и устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - меры по обеспечению безопасности персональных данных) для каждого из уровней защищенности персональных данных, установленных в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В настоящем документе не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

2. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система) обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

3. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской

Федерации от 1 ноября 2012 г. N1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда, применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

6. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

7. Меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328).

2. Типы угроз безопасности персональных данных.

8. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к

возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к настоящему документу.

8.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

8.2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

8.3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

8.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

8.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

8.6. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

8.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

8.8. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

8.9. Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

8.10. Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

8.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

8.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

8.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

8.14. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

8.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

9. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;

адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

10. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

11. В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, указанным в пункте 8 настоящего документа, могут применяться следующие меры:

проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

тестирование информационной системы на проникновения;

использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

12. При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

а) для обеспечения 1 и 2 уровней защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия информационной системы с информационнотелекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса

в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

б) для обеспечения 3 уровня защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

в) для обеспечения 4 уровня защищенности персональных данных применяются: .

средства вычислительной техники не ниже 6 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;

межсетевые экраны 5 класса.

Для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

13. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 настоящего документа.

3. Уровни защищенности персональных данных.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+

УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+

УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей персональных данных (ЗНИ)					

ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ. 2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных,хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или				

	переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ. 7	Защита информации о событиях безопасности	+	+	+	+
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.I	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий			+	+

	пользователей в информационной системе				
IX.Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ. 5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов),методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				

ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
ОДТ. 5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+

ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ. 8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и				

	иных внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС. 5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС. 7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				

ЗИС. 8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				

ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ. 5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+

УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

…….

1. 12 Лекция № 13 (2 часа).

Тема: «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"»

1.12.1 Вопросы лекции:

1. Общие положения.
2. Состав и содержание мер по обеспечению безопасности персональных данных.

…….

1.12.2 Краткое содержание вопросов:

1. Общие положения.

1. Настоящий документ разработан в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; 2011, N 23, ст. 3263; N 31, ст. 4701) и устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - меры по обеспечению безопасности персональных данных) для каждого из уровней защищенности персональных данных, установленных в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В настоящем документе не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

2. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система) обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

3. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской

Федерации от 1 ноября 2012 г. N1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда, применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

6. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

7. Меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328).

2. Состав и содержание мер по обеспечению безопасности персональных данных.

8. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к

возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к настоящему документу.

8.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

8.2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

8.3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

8.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

8.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

8.6. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

8.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

8.8. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

8.9. Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

8.10. Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

8.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

8.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

8.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

8.14. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

8.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

9. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;

адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

10. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

11. В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, указанным в пункте 8 настоящего документа, могут применяться следующие меры:

проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

тестирование информационной системы на проникновения;

использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

12. При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

а) для обеспечения 1 и 2 уровней защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия информационной системы с информационнотелекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса

в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

б) для обеспечения 3 уровня защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

в) для обеспечения 4 уровня защищенности персональных данных применяются: .

средства вычислительной техники не ниже 6 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;

межсетевые экраны 5 класса.

Для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

13. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 настоящего документа.

…….

1. 13 Лекция № 14 (2 часа).

Тема: «Нормативно-правовые, морально-этические, административные, физические и технические (программно-аппаратные) меры»

1.13.1 Вопросы лекции:

1. Нормативно-правовые меры.
2. Морально-этические меры.
3. Административные меры.

…….

1.13.2 Краткое содержание вопросов:

1. Нормативно-правовые меры.

Для обеспечения социальной безопасности в масштабах страны, региона, отрасли, организации, семьи или отдельной личности практикой выработаны самые разнообразные способы и средства:

- разведка (мониторинг) ситуации;
- уход от опасности, эвакуация;
- блокирование опасных факторов;
- ликвидация опасных факторов;
- силовое противодействие опасности;
- переговоры;
- совместное устранение причин опасности и иные меры.

Известен и общий алгоритм их применения – вначале необходимо выявить признаки социальных опасностей, затем спрогнозировать и оценить их развитие и последствия, выбрать стратегию поведения, затем на ее основе принять необходимые действия или управленческие решения и организовать их исполнение.

На уровне общества и государства, отдельной организации и даже отдельной семьи такое системное управление должно иметь свою методическую, нормативно-правовую, организационную и структурную основу, руководящие и контролирующие элементы, необходимые материальные ресурсы.

В данном разделе мы рассмотрим нормативно-правовое обеспечение вышеназванных мер защиты от социальных опасностей.

Законодательная основа обеспечения социальной безопасности

По каждому виду социальных угроз разрабатываются законы, которые принимаются Государственной Думой Федерального Собрания РФ, и региональные акты, принимаемые представительными органами субъектов Федерации. Для реализации требований законов принимаются подзаконные акты – Указы Президента РФ, Постановления Правительства, федеральные и местные целевые программы, определяющие порядок их исполнения.

Правовой основой обеспечениясоциальной безопасности в стране является *Конституция РФ* – основной закон государства. Законы и иные правовые акты, принимаемые в РФ, не должны противоречить Конституции РФ. Гарантом Конституции является Президент. Президент издает указы и распоряжения, обязательные для исполнения на всей территории Российской Федерации. Федеральные законы принимаются Государственной думой, рассматриваются Советом Федерации, подписываются и обнародуются Президентом.

Каждая статья Конституции, определяющая цели и принципы обеспечения безопасности личности, общества и государства подкрепляется соответствующим Федеральным законом или кодифицированным сборником законодательных норм – Кодексом РФ.

Во всех кодексах РФ: административном, гражданском, земельном, семейном, трудовом, уголовном и во всех иных обязательно присутствуют главы, регламентирующие соответствующие меры защиты от социальных опасностей.

По всем направлениям обеспечения защиты от опасностей социального характера ежегодно принимаются законы, постановления, о которых будет сказано в последующих разделах.

В качестве примера приведем некоторые законодательные акты и нормативно-правовые документы:

- Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 27.07.2006);

- ФЗ от 12 февраля 1998 г. № 28-ФЗ «О гражданской обороне» (в ред. от 22.08.2004);

- ФЗ от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» (в ред. от 27.07.2006);

- ФЗ от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (в ред. от 27.07.2006);

- ФЗ от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях» (в ред. от 6.07.2006);

- ФЗ от 5 марта 1992 г. № 2446-1 «О безопасности» (в ред. от 02.03.2007);

- ФЗ от 31 мая 1996 г. № 61-ФЗ «Об обороне» (в ред. от 26.06.2007);

- ФЗ от 8 января 1998 г. № 3-ФЗ «О санитарно – эпидемиологическом благополучии населения» (в ред. от 01.12.2007);

- ФЗ от 7 февраля 1992 г. № 2300-1 «О защите прав потребителей» (в ред. от 25.10.2007);

- ФЗ от 2 января 2000 г. № 29-ФЗ «О качестве и безопасности пищевых продуктов» (в ред. от 30.12.2006);

- ФЗ от 30 марта 1999 г. № 52-ФЗ «О наркотических средствах и психотропных веществах» (в ред. от 24.07.2007);

- ФЗ от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

- ФЗ от 24 июля 1999 г. № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних»;

- Положение о координации деятельности правоохранительных органов по борьбе с преступностью. Утверждено Указом Президента РФ от 18 апреля 1996 г. № 567;

- Примерные положения «О социально-реабилитационном центре для несовершеннолетних», «О социальном приюте для детей», «О центре помощи детям, оставшимся без попечения родителей», Утверждены постановлением Правительства РФ от 27 ноября 2000 г. № 896;

- Типовое положение о специальном учебно-воспитательном учреждении для детей и подростков с девиантным поведением. Утверждено постановлением Правительства РФ от 25 апреля 1995 г. № 420.

Далее рассмотрим региональные, федеральные и международные программы по обеспечению

2. Морально-этические меры.

Морально-этические меры защиты информации - традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний;

Нарушитель - это лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства;

Несанкционированное действие - действие субъекта в нарушение установленных в системе правил обработки информации;

Несанкционированный доступ - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;

Объект - пассивный компонент системы, единица ресурса информационной системы, доступ к которому регламентируется правилами разграничения доступа;

Объект защиты - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Организационно-правовые способы нарушения безопасности информации включают:

закупку несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;

невыполнение требований законодательства или нормативных актов и задержки в разработке и принятии необходимых нормативных правовых и технических документов в области безопасности информации.

Организационные меры защиты - это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации;

Организационный контроль эффективности защиты информации - проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Пароль - служебное слово, которое считается известным узкому кругу лиц (одному лицу) и используется для ограничения доступа к информации, в помещение, на территорию;

Пользователь - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе;

Правовые меры защиты информации - действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей;

Программно-математические способы нарушения безопасности информации включают:

внедрение программ-вирусов;

внедрение программных закладок как на стадии проектирования системы (в том числе путем заимствования "зараженного" закладками программного продукта), так и на стадии ее эксплуатации, позволяющих осуществить несанкционированный доступ или действия по отношению к информации и системам ее защиты (блокирование, обход и модификация систем защиты, извлечение, подмена идентификаторов и т.д.) и приводящих к компрометации системы защиты информации.

3. Административные меры.

Заключаются в определении процедур доступа к защищаемой информации и строгом их выполнении. Контроль над соблюдением установленного порядка возлагается на специально обученный персонал. Административные методы применялись многие века и диктовались здравым смыслом. Чтобы случайный человек не прочитал важный документ, такой документ нужно держать в охраняемом помещении. Чтобы передать секретное сообщение, его нужно посылать с курьером, который готов ценой собственной жизни защищать доверенную ему тайну. Чтобы из библиотеки не пропадали в неизвестном направлении книги, необходимо вести учет доступа к библиотечным ресурсам. Современные административные методы защиты информации весьма разнообразны. Например, при работе с документами, содержащими государственную

тайну, сначала необходимо оформить допуск к секретным документам. При получении документа и возврате его в хранилище в журнал регистрации заносятся соответствующие записи. Работа с документами разрешается только в специально оборудованном и сертифицированном помещений. На любом этапе известно лицо, несущее ответственность за целостность и секретность охраняемого документа. Схожие процедуры доступа к информации существуют и в различных организациях, где они определяются корпоративной политикой безопасности. Например, элементом политики безопасности может являться контроль вноса и выноса с территории организации носителей информации (бумажных, магнитных, оптических и др.). Административные методы защиты зачастую совмещаются с законодательными и могут устанавливать ответственность за попытки нарушения установленных процедур доступа.

…….

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Не предусмотрено РУП.

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1 Практическое занятие № 1-2 (4 часа).

Тема: «Основные понятия, термины и определения»

3.1.1 Задание для работы:

1. Введение в проблемы информационной безопасности.
2. Основные понятия, термины и определения.

…….

3.1.2 Краткое описание проводимого занятия:

1. Введение в проблемы информационной безопасности.

- Что такое информационная безопасность.
- Уровни решения проблемы информационной безопасности.
- Содержание основных законов Российской Федерации в сфере компьютерного права.
- Уровни защиты информации.
- Меры защиты информационной безопасности.
- Угрозы для информационной безопасности, связанные с подключением к глобальной компьютерной сети Интернет и меры безопасного использования сервисов Интернета.

В связи с массовой информатизацией современного общества все большую актуальность приобретает знание нравственно-этических норм и правовых основ использования средств новых информационных технологий в повседневной практической деятельности. Наглядными примерами, иллюстрирующими необходимость защиты информации и обеспечения информационной безопасности, являются участившиеся сообщения о компьютерных «взломах» банков, росте компьютерного пиратства, распространении компьютерных вирусов.

Число компьютерных преступлений растет, также увеличиваются масштабы компьютерных злоупотреблений. Умышленные компьютерные преступления составляют заметную часть преступлений, но злоупотреблений компьютерами и ошибок еще больше.

Основной причиной потерь, связанных с компьютерами, является недостаточная образованность в области безопасности.

Под информационной безопасностью понимается защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации.

Цель информационной безопасности - обезопасить ценности системы, защитить и гарантировать точность и целостность информации и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена.

На практике важнейшими являются три аспекта информационной безопасности:

- доступность (возможность за разумное время получить требуемую информационную услугу);
- целостность (ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения).

Кроме того, использование информационных систем должно производиться в соответствии с существующим законодательством. Данное положение, разумеется, применимо к любому виду деятельности, однако информационные технологии специфичны в том отношении, что развиваются исключительно быстрыми темпами. Почти всегда законодательство отстает от потребностей практики, и это создает в обществе определенную напряженность. Для информационных технологий подобное отставание законов, нормативных актов, национальных и отраслевых стандартов оказывается особенно болезненным.

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно разделить на четыре уровня:

1. законодательный (законы, нормативные акты, стандарты и т.п.);
2. административный (действия общего характера, предпринимаемые руководством организации);
3. процедурный (конкретные меры безопасности, имеющие дело с людьми);
4. программно-технический (конкретные технические меры).

2. Основные понятия, термины и определения.

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

- конфиденциальность (англ. *confidentiality*) — состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право;
- целостность (англ. *integrity*) — избежание несанкционированной модификации информации;
- доступность (англ. *availability*) — избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

- неотказуемость или апеллируемость (англ. *non-repudiation*) — способность удостоверять имевшее место действие или событие так, что эти события или действия не могли быть позже отвергнуты;
- подотчётность (англ. *accountability*) — свойство, обеспечивающее однозначное прослеживание действий любого логического объекта.;
- достоверность (англ. *reliability*) — свойство соответствия предусмотренному поведению или результату;
- аутентичность или подлинность (англ. *authenticity*) — свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Системный подход к описанию информационной безопасности предлагает выделить следующие составляющие информационной безопасности[9]:

5. Законодательная, нормативно-правовая и научная база.
6. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
7. Организационно-технические и режимные меры и методы (Политика информационной безопасности).
8. Программно-технические способы и средства обеспечения информационной безопасности.

Ниже в данном разделе подробно будет рассмотрена каждая из составляющих информационной безопасности.
Целью реализации информационной безопасности какого-либо объекта является построение Системы обеспечения информационной безопасности данного объекта (СОИБ). Для построения и эффективной эксплуатации СОИБ необходимо[3]:

- выявить требования защиты информации, специфические для данного объекта защиты;
- учесть требования национального и международного Законодательства;
- использовать наработанные практики (стандарты, методологии) построения подобных СОИБ;
- определить подразделения, ответственные за реализацию и поддержку СОИБ;
- распределить между подразделениями области ответственности в осуществлении требований СОИБ;

- на базе управления рисками информационной безопасности определить общие положения, технические и организационные требования, составляющие Политику информационной безопасности объекта защиты;
- реализовать требования Политики информационной безопасности, внедрив соответствующие программно-технические способы и средства защиты информации;
- реализовать Систему менеджмента (управления) информационной безопасности (СМИБ);
- используя СМИБ организовать регулярный контроль эффективности СОИБ и при необходимости пересмотр и корректировку СОИБ и СМИБ.

Как видно из последнего этапа работ, процесс реализации СОИБ непрерывный и циклично (после каждого пересмотра) возвращается к первому этапу, повторяя последовательно все остальные. Так СОИБ корректируется для эффективного выполнения своих задач защиты информации и соответствия новым требованиям постоянно обновляющейся информационной системы.

3.1.3 Результаты и выводы:

Студенты изучили основные понятия, термины и определения информационной безопасности.

3.2 Практическое занятие № 3 (2 часа).

Тема: «Основы государственной политики в области информационной безопасности»

3.2.1 Задание для работы:

1. Основы государственной политики в области информационной безопасности.
2. Стратегия национальной безопасности Российской Федерации.

…….

3.2.2 Краткое описание проводимого занятия:

1. Основы государственной политики в области информационной безопасности.

1. Настоящие Основы являются документом стратегического планирования Российской Федерации.

2. Настоящими Основами определяются основные угрозы в области международной информационной безопасности, цель, задачи и приоритетные направления государственной политики Российской Федерации в области международной информационной безопасности (далее - государственная политика Российской Федерации), а также механизмы их реализации.

3. Нормативную правовую базу настоящих Основ составляют Конституция Российской Федерации, международные договоры Российской Федерации в области международной информационной безопасности, федеральные законы, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, иные нормативные правовые акты Российской Федерации.

4. Настоящие Основы конкретизируют отдельные положения Стратегии национальной безопасности Российской Федерации до 2020 года, Доктрины информационной безопасности Российской Федерации, Концепции внешней политики Российской Федерации и других документов стратегического планирования Российской Федерации.

5. Настоящие Основы предназначены:

а) для продвижения на международной арене российских инициатив в области формирования системы международной информационной безопасности, включая совершенствование правового, организационного и иных видов ее обеспечения;

б) для формирования межгосударственных целевых программ в области международной информационной безопасности, в осуществлении которых участвует Российская Федерация, а также государственных и федеральных целевых программ в данной области;

в) для организации межведомственного взаимодействия при реализации государственной политики Российской Федерации в области международной информационной безопасности;

г) для достижения и поддержания технологического паритета с ведущими мировыми державами за счет более широкого использования информационных и коммуникационных технологий в реальном секторе экономики.

6. Под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

7. Под системой международной информационной безопасности понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства. Система международной информационной безопасности призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве. Сотрудничество в области формирования системы международной информационной безопасности отвечает национальным интересам Российской Федерации и способствует укреплению ее национальной безопасности.

8. Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

II. Цель и задачи государственной политики Российской Федерации

9. Цель государственной политики Российской Федерации заключается в содействии установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности.

10. Достижению цели государственной политики Российской Федерации будет способствовать участие Российской Федерации в решении следующих задач:

а) формирование системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях;

б) создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

в) формирование механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях;

г) создание условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств;

д) повышение эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий;

е) создание условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами.

III. Основные направления государственной политики Российской Федерации

11. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях, являются:

а) создание условий для продвижения на международной арене российской инициативы в необходимости разработки и принятия государствами - членами Организации Объединенных Наций Конвенции об обеспечении международной информационной безопасности;

б) содействие закреплению российских инициатив в области формирования системы международной информационной безопасности в итоговых документах, изданных по результатам работы Группы правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также содействие выработке под эгидой Организации Объединенных Наций правил поведения в области обеспечения международной информационной безопасности, отвечающих национальным интересам Российской Федерации;

в) проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и планов действий с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС, странами - членами Азиатско-тихоокеанского экономического сотрудничества, странами - членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами в области международной информационной безопасности;

г) продвижение на международной арене российской инициативы в интернационализации управления информационно-телекоммуникационной сетью «Интернет» и увеличение в этом контексте роли Международного союза электросвязи;

д) организационно-штатное укрепление структурных подразделений федеральных органов исполнительной власти, участвующих в реализации государственной политики Российской Федерации, а также совершенствование координации деятельности федеральных органов исполнительной власти в данной области;
е) создание механизма участия российского экспертного сообщества в совершенствовании аналитического и научно-методического обеспечения продвижения российских инициатив в области формирования системы международной информационной безопасности;
ж) создание условий для заключения между Российской Федерацией и иностранными государствами международных договоров о сотрудничестве в области обеспечения международной информационной безопасности;
з) усиление взаимодействия в рамках Соглашения между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности и содействие расширению состава участников указанного Соглашения;
и) использование научного, исследовательского и экспертного потенциала Организации Объединенных Наций, других международных организаций для продвижения российских инициатив в области формирования системы международной информационной безопасности.
12. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий, способствующих снижению риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности, являются:
а) развитие диалога с заинтересованными государствами о национальных подходах к противодействию вызовам и угрозам, возникающим в связи с масштабным использованием информационных и коммуникационных технологий в военно-политических целях;
б) участие в выработке на двустороннем и многостороннем уровнях мер по укреплению доверия в области противодействия угрозам использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии;
в) содействие развитию региональных систем и формированию глобальной системы международной информационной безопасности на основе общепризнанных принципов и норм международного права (уважение государственного суверенитета, невмешательство во внутренние дела других государств, неприменение силы и угрозы силой в международных отношениях, право на индивидуальную и коллективную самооборону, уважение прав и основных свобод человека);
г) содействие подготовке и принятию государствами - членами Организации Объединенных Наций международных правовых актов, регламентирующих применение принципов и норм международного гуманитарного права в сфере использования информационных и коммуникационных технологий;
д) создание условий для установления международного правового режима нераспространения информационного оружия.
13. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях, являются:
а) развитие сотрудничества с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности,

государствами - участниками БРИКС, способствующего предупреждению, выявлению, пресечению, раскрытию и расследованию актов деструктивного воздействия на элементы национальной критической информационной инфраструктуры, минимизации последствий реализации таких актов, а также противодействию использования информационно-телекоммуникационной сети «Интернет» и других информационно-телекоммуникационных сетей в целях пропаганды терроризма и привлечения к террористической деятельности новых сторонников;
б) содействие подготовке и принятию государствами - членами Организации Объединенных Наций акта, определяющего порядок обмена информацией о передовых практиках в области обеспечения безопасности функционирования элементов критической информационной инфраструктуры.
14. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств, являются:
а) участие в разработке и реализации межгосударственной системы мер по противодействию указанным угрозам;
б) содействие созданию международного механизма постоянного контроля за недопущением использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств.
15. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по повышению эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий, являются:
а) продвижение на международной арене российской инициативы в необходимости разработки и принятия под эгидой Организации Объединенных Наций Конвенции о сотрудничестве в сфере противодействия информационной преступности, а также активизация работы с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС по поддержке данной инициативы;
б) развитие сотрудничества в сфере противодействия информационной преступности с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС, странами -членами Азиатско-тихоокеанского экономического сотрудничества, странами - членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами;
в) повышение эффективности информационного обмена между правоохранительными органами государств в ходе расследования преступлений в сфере использования информационных и коммуникационных технологий;
г) совершенствование механизма обмена информацией о методиках расследования и судебной практике рассмотрения дел о преступлениях в сфере использования информационных и коммуникационных технологий.
16. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами, являются:
а) содействие разработке и реализации международных программ, способствующих

преодолению информационного неравенства между развитыми и развивающимися странами;
б) содействие развитию национальных информационных инфраструктур и участию государств мирового сообщества в процессах создания и использования глобальных информационных сетей и систем.

IV. Механизмы реализации государственной политики Российской Федерации

17. Государственная политика Российской Федерации реализуется федеральными органами исполнительной власти и надзорными органами в соответствии с предметами их ведения при выполнении соответствующих межгосударственных целевых программ, в осуществлении которых участвует Российская Федерация, государственных и федеральных целевых программ, в том числе в рамках государственно-частного партнерства.

18. Подготовка предложений Президенту Российской Федерации по реализации основных направлений государственной политики Российской Федерации осуществляется рабочими органами Совета Безопасности Российской Федерации во взаимодействии с заинтересованными самостоятельными подразделениями Администрации Президента Российской Федерации, федеральными органами исполнительной власти и организациями.

19. Общая координация деятельности федеральных органов исполнительной власти, связанной с реализацией государственной политики Российской Федерации, а также с продвижением согласованной позиции Российской Федерации по этому вопросу на международной арене, осуществляется Министерством иностранных дел Российской Федерации.

* * *

20. Интенсивное развитие информационных и коммуникационных технологий, их широкое применение во всех сферах деятельности человека создали условия для формирования глобальной информационной инфраструктуры, которая предоставила качественно новые возможности социализации людей, их общения и доступа к накопленным человечеством знаниям.
В современном обществе информационные и коммуникационные технологии являются основным фактором, определяющим уровень социально-экономического развития и состояние национальной безопасности.
Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года призваны способствовать активизации внешней политики Российской Федерации на пути достижения согласия и учета взаимных интересов в процессе интернационализации глобального информационного пространства.

2. Стратегия национальной безопасности Российской Федерации.

1. Общие положения

1. Настоящая Стратегия является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу.

2. Правовую основу настоящей Стратегии составляют Конституция Российской Федерации, федеральные законы от 28 декабря 2010 г. N 390-ФЗ "О безопасности" и от 28 июня 2014 г. N 172-ФЗ "О стратегическом планировании в Российской Федерации",

другие федеральные законы, нормативные правовые акты Президента Российской Федерации.

3. Настоящая Стратегия призвана консолидировать усилия федеральных органов государственной власти, других государственных органов, органов государственной власти субъектов Российской Федерации (далее - органы государственной власти), органов местного самоуправления, институтов гражданского общества по созданию благоприятных внутренних и внешних условий для реализации национальных интересов и стратегических национальных приоритетов Российской Федерации.

4. Настоящая Стратегия является основой для формирования и реализации государственной политики в сфере обеспечения национальной безопасности Российской Федерации.

5. Настоящая Стратегия основана на неразрывной взаимосвязи и взаимозависимости национальной безопасности Российской Федерации и социально-экономического развития страны.

6. В настоящей Стратегии используются следующие основные понятия:

национальная безопасность Российской Федерации (далее - национальная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее - граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности;

национальные интересы Российской Федерации (далее - национальные интересы) объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития;

угроза национальной безопасности - совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам;

обеспечение национальной безопасности - реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов;

стратегические национальные приоритеты Российской Федерации (далее - стратегические национальные приоритеты) - важнейшие направления обеспечения национальной безопасности;

система обеспечения национальной безопасности совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной

безопасности органов государственной власти и органов местного самоуправления и находящихся в их распоряжении инструментов.

II. Россия в современном мире

7. Государственная политика в сфере обеспечения национальной безопасности и социально-экономического развития Российской Федерации способствует реализации стратегических национальных приоритетов и эффективной защите национальных интересов. В настоящее время создана устойчивая основа для дальнейшего наращивания экономического, политического, военного и духовного потенциалов Российской Федерации, повышения ее роли в формирующемся полицентричном мире.

8. Россия продемонстрировала способность к обеспечению суверенитета, независимости, государственной и территориальной целостности, защиты прав соотечественников за рубежом. Возросла роль Российской Федерации в решении важнейших международных проблем, урегулировании военных конфликтов, обеспечении стратегической стабильности и верховенства международного права в межгосударственных отношениях.

9. Экономика России проявила способность к сохранению и укреплению своего потенциала в условиях нестабильности мировой экономики и применения ограничительных экономических мер, введенных рядом стран против Российской Федерации.

10. Позитивные тенденции наметились в решении задач укрепления здоровья граждан. Отмечаются естественный прирост населения, увеличение средней продолжительности жизни.

11. Возрождаются традиционные российские духовно-нравственные ценности. У подрастающего поколения формируется достойное отношение к истории России. Происходит консолидация гражданского общества вокруг общих ценностей, формирующих фундамент государственности, таких как свобода и независимость России, гуманизм, межнациональный мир и согласие, единство культур многонационального народа Российской Федерации, уважение семейных и конфессиональных традиций, патриотизм.

12. Укрепление России происходит на фоне новых угроз национальной безопасности, имеющих комплексный взаимосвязанный характер. Проведение Российской Федерацией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых делах. Реализуемая ими политика сдерживания России предусматривает оказание на нее политического, экономического, военного и информационного давления.

13. Процесс формирования новой полицентричной модели мироустройства сопровождается ростом глобальной и региональной нестабильности. Обостряются противоречия, связанные с неравномерностью мирового развития, углублением разрыва между уровнями благосостояния стран, борьбой за ресурсы, доступом к рынкам сбыта, контролем над транспортными артериями.

Конкуренция между государствами все в большей степени охватывает ценности и

модели общественного развития, человеческий, научный и технологический потенциалы. Особое значение в этом процессе приобретает лидерство в освоении ресурсов Мирового океана и Арктики. В борьбе за влияние на международной арене задействован весь спектр политических, финансово-экономических и информационных инструментов. Все активнее используется потенциал специальных служб.

14. В международных отношениях не снижается роль фактора силы. Стремление к наращиванию и модернизации наступательного вооружения, созданию и развертыванию его новых видов ослабляет систему глобальной безопасности, а также систему договоров и соглашений в области контроля над вооружением. В Евро-Атлантическом, Евразийском и Азиатско-Тихоокеанском регионах не соблюдаются принципы равной и неделимой безопасности. В соседних с Россией регионах развиваются процессы милитаризации и гонки вооружений.

15. Наращивание силового потенциала Организации Североатлантического договора (НАТО) и наделение ее глобальными функциями, реализуемыми в нарушение норм международного права, активизация военной деятельности стран блока, дальнейшее расширение альянса, приближение его военной инфраструктуры к российским границам создают угрозу национальной безопасности.

Возможности поддержания глобальной и региональной стабильности существенно снижаются при размещении в Европе, Азиатско-Тихоокеанском регионе и на Ближнем Востоке компонентов системы противоракетной обороны США, в условиях практической реализации концепции "глобального удара", развертывания стратегических неядерных систем высокоточного оружия, а также в случае размещения оружия в космосе.

16. Сохраняющийся блоковый подход к решению международных проблем не способствует противодействию всему спектру современных вызовов и угроз. Активизация миграционных потоков из стран Африки и Ближнего Востока в Европу показала несостоятельность региональной системы безопасности в Евро-Атлантическом регионе, построенной на основе НАТО и Европейского союза.

17. Позиция Запада, направленная на противодействие интеграционным процессам и создание очагов напряженности в Евразийском регионе, оказывает негативное влияние на реализацию российских национальных интересов. Поддержка США и Европейским союзом антиконституционного государственного переворота на Украине привела к глубокому расколу в украинском обществе и возникновению вооруженного конфликта. Укрепление крайне правой националистической идеологии, целенаправленное формирование у украинского населения образа врага в лице России, неприкрытая ставка на силовое решение внутригосударственных противоречий, глубокий социально-экономический кризис превращают Украину в долгосрочный очаг нестабильности в Европе и непосредственно у границ России.

18. Практика свержения легитимных политических режимов, провоцирования внутригосударственных нестабильности и конфликтов получает все более широкое распространение. Наряду с сохраняющимися очагами напряженности на Ближнем и Среднем Востоке, в Африке, Южной Азии, на Корейском полуострове появляются новые "горячие точки", расширяются зоны, не контролируемые властями каких-либо государств. Территории вооруженных конфликтов становятся базой для распространения терроризма, межнациональной розни, религиозной вражды, иных проявлений экстремизма. Появление террористической организации, объявившей себя

"Исламским государством", и укрепление ее влияния стали результатом политики двойных стандартов, которой некоторые государства придерживаются в области борьбы с терроризмом.

19. Сохраняется риск увеличения числа стран - обладателей ядерного оружия, распространения и использования химического оружия, а также неопределенность относительно фактов обладания иностранными государствами биологическим оружием, наличия у них потенциала для его разработки и производства. На территориях соседних с Россией государств расширяется сеть военнобиологических лабораторий США.

20. Критическое состояние физической сохранности опасных объектов и материалов, особенно в государствах с нестабильной внутриполитической ситуацией, неконтролируемое распространение обычного вооружения повышают вероятность их попадания в руки террористов.

21. Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории.

22. Появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. Обостряются угрозы, связанные с неконтролируемой и незаконной миграцией, торговлей людьми, наркоторговлей и другими проявлениями транснациональной организованной преступности.

23. Осложняются мировая демографическая ситуация, проблемы окружающей среды и продовольственной безопасности. Более ощутимыми становятся дефицит пресной воды, последствия изменения климата. Получают распространение эпидемии, многие из которых вызваны новыми, неизвестными ранее вирусами.

24. Возрастающее влияние политических факторов на экономические процессы, а также попытки применения отдельными государствами экономических методов, инструментов финансовой, торговой, инвестиционной и технологической политики для решения своих геополитических задач ослабляют устойчивость системы международных экономических отношений. На фоне структурных дисбалансов в мировой экономике и финансовой системе, растущей суверенной задолженности, волатильности рынка энергоресурсов сохраняется высокий риск повторения масштабных финансово-экономических кризисов.

25. Государства в качестве реакции на рост международной нестабильности все чаще берут на себя ответственность за дела в своих регионах. Региональные и субрегиональные торговые и иные экономические соглашения становятся одним из важнейших средств защиты от кризисных явлений. Повышается интерес к использованию региональных валют.

26. Для предотвращения угроз национальной безопасности Российская Федерация сосредоточивает усилия на укреплении внутреннего единства российского общества, обеспечении социальной стабильности, межнационального согласия и религиозной терпимости, устранении структурных дисбалансов в экономике и ее модернизации, повышении обороноспособности страны.

27. В целях защиты национальных интересов Россия проводит открытую, рациональную и прагматичную внешнюю политику, исключающую затратную конфронтацию (в том числе новую гонку вооружений).

28. Российская Федерация выстраивает международные отношения на принципах международного права, обеспечения надежной и равной безопасности государств, взаимного уважения народов, сохранения многообразия их культур, традиций и интересов. Россия заинтересована в развитии взаимовыгодного и равноправного торгово-экономического сотрудничества с иностранными государствами, является ответственным участником многосторонней торговой системы. Цель Российской Федерации заключается в приобретении как можно большего числа равноправных партнеров в различных частях мира.

29. В области международной безопасности Россия сохраняет приверженность использованию прежде всего политических и правовых инструментов, механизмов дипломатии и миротворчества. Применение военной силы для защиты национальных интересов возможно только в том случае, если все принятые меры ненасильственного характера оказались неэффективными.

III. Национальные интересы и стратегические национальные приоритеты

30. Национальными интересами на долгосрочную перспективу являются:

укрепление обороны страны, обеспечение незыблемости конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации;
укрепление национального согласия, политической и социальной стабильности, развитие демократических институтов, совершенствование механизмов взаимодействия государства и гражданского общества;
повышение качества жизни, укрепление здоровья населения, обеспечение стабильного демографического развития страны;
сохранение и развитие культуры, традиционных российских духовно-нравственных ценностей;
повышение конкурентоспособности национальной экономики;
закрепление за Российской Федерацией статуса одной из лидирующих мировых держав, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях полицентричного мира.

31. Обеспечение национальных интересов осуществляется посредством реализации следующих стратегических национальных приоритетов:

оборона страны;
государственная и общественная безопасность;
повышение качества жизни российских граждан;
экономический рост;
наука, технологии и образование;
здравоохранение;
культура;
экология живых систем и рациональное природопользование;
стратегическая стабильность и равноправное стратегическое партнерство.

IV. Обеспечение национальной безопасности

32. Состояние национальной безопасности напрямую зависит от степени реализации стратегических национальных приоритетов и эффективности функционирования системы обеспечения национальной безопасности.

Оборона страны

33. Стратегическими целями обороны страны являются создание условий для мирного и динамичного социально-экономического развития Российской Федерации, обеспечение ее военной безопасности.

34. Достижение стратегических целей обороны страны осуществляется в рамках реализации военной политики путем стратегического сдерживания и предотвращения военных конфликтов, совершенствования военной организации государства, форм и способов применения Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, повышения мобилизационной готовности Российской Федерации и готовности сил и средств гражданской обороны.

35. Основные положения военной политики и задачи военно-экономического обеспечения обороны страны, военные опасности и военные угрозы определяются Военной доктриной Российской Федерации.

36. В целях обеспечения стратегического сдерживания и предотвращения военных конфликтов разрабатываются и реализуются взаимосвязанные политические, военные, военно-технические, дипломатические, экономические, информационные и иные меры, направленные на предотвращение применения военной силы в отношении России, защиту ее суверенитета и территориальной целостности. Стратегическое сдерживание и предотвращение военных конфликтов осуществляются путем поддержания потенциала ядерного сдерживания на достаточном уровне, а Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов в заданной степени готовности к боевому применению.

37. Совершенствование военной организации государства осуществляется на основе своевременного выявления существующих и перспективных военных опасностей и военных угроз, сбалансированного развития компонентов военной организации, наращивания оборонного потенциала, оснащения Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов современными вооружением, военной и специальной техникой, инновационного развития оборонно-промышленного комплекса Российской Федерации.

38. Совершенствование форм и способов применения Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов предусматривает своевременный учет тенденций изменения характера современных войн и вооруженных конфликтов, создание условий для наиболее полной реализации боевых возможностей войск (сил), выработку требований к перспективным формированиям и новым средствам вооруженной борьбы.

39. Повышение мобилизационной готовности Российской Федерации осуществляется путем совершенствования планирования мер по обеспечению мобилизационной

подготовки и мобилизации в Российской Федерации и их реализации в необходимом объеме, своевременного обновления и поддержания на достаточном уровне военно-технического потенциала военной организации государства. Важнейшими направлениями совершенствования мобилизационной подготовки являются подготовка экономики Российской Федерации, экономики субъектов Российской Федерации, экономики муниципальных образований, подготовка органов государственной власти, органов местного самоуправления и организаций, Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов к выполнению задач в соответствии с их предназначением и удовлетворению потребностей государства и нужд населения в военное время.

40. Готовность сил и средств гражданской обороны обеспечивается заблаговременно путем проведения мероприятий по подготовке к защите и по защите населения, материальных и культурных ценностей на территории Российской Федерации от опасностей, возникающих при военных конфликтах или вследствие этих конфликтов, а также при чрезвычайных ситуациях природного и техногенного характера.

41. Обеспечение обороны страны осуществляется на основании принципов рациональной достаточности и эффективности, в том числе путем применения методов и средств невоенного реагирования, механизмов дипломатии и миротворчества, расширения международного военного и военно-технического сотрудничества, контроля над вооружением и использования других международно-правовых инструментов.

Государственная и общественная безопасность

42. Стратегическими целями государственной и общественной безопасности являются защита конституционного строя, суверенитета, государственной и территориальной целостности Российской Федерации, основных прав и свобод человека и гражданина, сохранение гражданского мира, политической и социальной стабильности в обществе. защита населения и территорий от чрезвычайных ситуаций природного и техногенного характера.

43. Основными угрозами государственной и общественной безопасности являются:

разведывательная и иная деятельность специальных служб и организаций иностранных государств, отдельных лиц, наносящая ущерб национальным интересам;

деятельность террористических и экстремистских организаций, направленная на насильственное изменение конституционного строя Российской Федерации, дестабилизацию работы органов государственной власти, уничтожение или нарушение функционирования военных и промышленных объектов, объектов жизнеобеспечения населения, транспортной инфраструктуры, устрашение населения, в том числе путем завладения оружием массового уничтожения, радиоактивными, отравляющими, токсичными, химически и биологически опасными веществами, совершения актов ядерного терроризма, нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации;

деятельность радикальных общественных объединений и группировок, использующих националистическую и религиозно-экстремистскую идеологию, иностранных и международных неправительственных организаций, финансовых и экономических структур, а также частных лиц, направленная на нарушение единства и

территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране, включая инспирирование "цветных революций", разрушение традиционных российских духовно-нравственных ценностей;

деятельность преступных организаций и группировок, в том числе транснациональных, связанная с незаконным оборотом наркотических средств и психотропных веществ, оружия, боеприпасов, взрывчатых веществ, организацией незаконной миграции и торговлей людьми;

деятельность, связанная с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе;

преступные посягательства, направленные против личности, собственности, государственной власти, общественной и экономической безопасности;

коррупция;

стихийные бедствия, аварии и катастрофы, в том числе связанные с глобальным изменением климата, ухудшением технического состояния объектов инфраструктуры и возникновением пожаров.

44. Главными направлениями обеспечения государственной и общественной безопасности являются усиление роли государства в качестве гаранта безопасности личности и прав собственности, совершенствование правового регулирования предупреждения преступности (в том числе в информационной сфере), коррупции, терроризма и экстремизма, распространения наркотиков и борьбы с такими явлениями, развитие взаимодействия органов обеспечения государственной безопасности и правопорядка с гражданским обществом, повышение доверия граждан к правоохранительной и судебной системам Российской Федерации, эффективности защиты прав и законных интересов российских граждан за рубежом, расширение международного сотрудничества в области государственной и общественной безопасности.

45. Обеспечение государственной и общественной безопасности осуществляется путем повышения эффективности деятельности правоохранительных органов и специальных служб, органов государственного контроля (надзора), совершенствования единой государственной системы профилактики преступности, в первую очередь среди несовершеннолетних, и иных правонарушений (включая мониторинг и оценку эффективности правоприменительной практики), разработки и использования специальных мер, направленных на снижение уровня криминализации общественных отношений.

46. Особое внимание уделяется искоренению причин и условий, порождающих коррупцию, которая является препятствием устойчивому развитию Российской Федерации и реализации стратегических национальных приоритетов. В этих целях реализуются Национальная стратегия противодействия коррупции и национальные планы противодействия коррупции, в обществе формируется атмосфера неприемлемости данного явления, повышается уровень ответственности за коррупционные преступления, совершенствуется правоприменительная практика в

указанной области.

47. В целях обеспечения государственной и общественной безопасности:

совершенствуются структура и деятельность федеральных органов исполнительной власти, развивается система выявления, предупреждения и пресечения разведывательной и иной деструктивной деятельности специальных служб и организаций иностранных государств, наносящей ущерб национальным интересам, актов терроризма, проявлений религиозного радикализма, национализма, сепаратизма, иных форм экстремизма, организованной преступности и других преступных посягательств на конституционный строй Российской Федерации, права и свободы человека и гражданина, государственную и частную собственность, общественный порядок и общественную безопасность;

создаются механизмы предупреждения и нейтрализации социальных и межнациональных конфликтов, а также противодействия участию российских граждан в деятельности преступных и террористических группировок за рубежом;

укрепляется режим безопасного функционирования, повышается уровень антитеррористической защищенности организаций оборонно-промышленного, ядерного, химического, топливно-энергетического комплексов страны, объектов жизнеобеспечения населения, транспортной инфраструктуры, других критически важных и потенциально опасных объектов;
совершенствуется система выявления и анализа угроз в информационной сфере, противодействия им;
принимаются меры для повышения защищенности граждан и общества от деструктивного информационного воздействия со стороны экстремистских и террористических организаций, иностранных специальных служб и пропагандистских структур;
осуществляется комплексное развитие правоохранительных органов и специальных служб, укрепляются социальные гарантии их сотрудникам, совершенствуется научно-техническая поддержка правоохранительной деятельности, принимаются на вооружение перспективные специальные средства и техника, развивается система профессиональной подготовки специалистов в области обеспечения государственной и общественной безопасности;
повышается социальная ответственность органов обеспечения государственной и общественной безопасности.

3.2.3 Результаты и выводы:

Студенты изучили основы государственной политики в области информационной безопасности.

3.3 Практическое занятие № 4 (2 часа).

Тема: «Аттестация объектов информатизации по требованиям безопасности информации»

3.3.1 Задание для работы:

1. Общие положения.
2. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.
3. Порядок проведения аттестации и контроля.

…….

3.3.2 Краткое описание проводимого занятия:

1. Общие положения.

1.1. Настоящее Положение устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

1.2. Положение разработано в соответствии с Законами Российской Федерации "О сертификации продукции и услуг" и "О государственной тайне", "Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам", "Положением о государственном лицензировании деятельности в области защиты информации", "Положением о сертификации средств защиты информации по требованиям безопасности информации", "Системой сертификации ГОСТ Р".

1.3. Система аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации) является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном Госстандартом России порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации (далее - федеральный орган по сертификации и аттестации), которым является Гостехкомиссия России.

1.4. Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России.

Наличие на объекте информатизации действующего "Аттестата соответствия" дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в "Аттестате соответствия".

1.5. Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.

В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

1.6. При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и

облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

1.7. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

1.8. Аттестация проводится органом по аттестации в установленном настоящим Положением порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;

- предварительное ознакомление с аттестуемым объектом информатизации;

- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;

- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

1.9. Органы по аттестации аккредитуются Гостехкомиссией России. Правила аккредитации определяются действующим в системе "Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации".

Гостехкомиссия России может передавать права на аккредитацию отраслевых (ведомственных) органов по аттестации другим органам государственной власти.

1.10. Расходы по проведению всех видов работ и услуг по обязательной и добровольной аттестации объектов информатизации оплачивают заявители.

Оплата работ по обязательной аттестации производится в соответствии с договором по утвержденным расценкам, а при их отсутствии - по договорной цене в порядке, установленном Гостехкомиссией России по согласованию с Министерством финансов Российской Федерации.

Расходы по проведению всех видов работ и услуг по аттестации объектов информатизации оплачивают заявители за счет финансовых средств, выделенных на разработку (доработку) и введение в действие защищаемого объекта информатизации.

1.11. Органы по аттестации объектов информатизации несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонент.

2. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.

2.1. Организационную структуру системы аттестации объектов информатизации образуют:

- федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации - Гостехкомиссия России;

- органы по аттестации объектов информатизации по требованиям безопасности информации;

- испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;

- заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

2.2. Федеральный орган по сертификации и аттестации осуществляет следующие функции:

- организует обязательную аттестацию объектов информатизации;

- создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;

- устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;

- организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;

- аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;

- осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;

- рассматривает апелляции, возникающие в процессе аттестации объектов информатизации и контроля за эксплуатацией аттестованных объектов информатизации;

- организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

2.3. Органы по аттестации объектов информатизации аккредитуются Гостехкомиссией России и получают от нее лицензию на право проведения аттестации объектов информатизации.

Такими органами могут быть отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры Гостехкомиссии России.

2.4. Органы по аттестации:

- аттестуют объекты информатизации и выдают "Аттестаты соответствия";

- осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией;

- отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";

- формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;

- ведут информационную базу аттестованных этим органом объектов информатизации;

- осуществляют взаимодействие с Гостехкомиссией России и ежеквартально информируют его о своей деятельности в области аттестации.

2.5. Испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации по заказам заявителей проводят испытания несертифицированной продукции, используемой на объекте информатики, подлежащем обязательной аттестации, в соответствии с "Положением о сертификации средств защиты информации по требованиям безопасности информации".

2.6. Заявители:

- проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;

- привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;

- предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;

- привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;

- осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";

- извещают орган по аттестации, выдавший "Аттестат соответствия", о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");

- предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

3. Порядок проведения аттестации и контроля.

3.1. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

- подачу и рассмотрение заявки на аттестацию;

- предварительное ознакомление с аттестуемым объектом;

- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);

- разработка программы и методики аттестационных испытаний;

- заключение договоров на аттестацию;

- проведение аттестационных испытаний объекта информатизации;

- оформление, регистрация и выдача "Аттестата соответствия";

- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;

- рассмотрение апелляций.

3.2. Подача и рассмотрение заявки на аттестацию

3.2.1. Заявитель для получения "Аттестата соответствия" заблаговременно направляет в орган по аттестации заявку на проведение аттестации с исходными данными по аттестуемому объекту информатизации по форме, приведенной в приложении 1.

3.2.2. Орган по аттестации в месячный срок рассматривает заявку и на основании анализа исходных данных выбирает схему аттестации, согласовывает ее с заявителем и принимает решение о проведении аттестации объекта информатизации.

3.3. Предварительное ознакомление с аттестуемым объектом

При недостаточности исходных данных по аттестуемому объекту информатизации в схему аттестации включаются работы по предварительному ознакомлению с аттестуемым объектом, проводимые до этапа аттестационных испытаний.

3.4. Испытания несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте информатизации

3.4.1. При использовании на аттестуемом объекте информатизации несертифицированных средств и систем защиты информации в схему аттестации могут быть включены работы по их испытаниям в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации или непосредственно на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств.

3.4.2. Испытания отдельных несертифицированных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации проводятся до аттестационных испытаний объектов информатизации.

В этом случае заявителем к началу аттестационных испытаний должны быть представлены заключения органов по сертификации средств защиты информации по требованиям безопасности информации и сертификаты.

3.5. Разработка программы и методики аттестационных испытаний

3.5.1. По результатам рассмотрения заявки и анализа исходных данных, а также предварительного ознакомления с аттестуемым объектом органом по аттестации разрабатываются программа аттестационных испытаний, предусматривающая перечень работ и их продолжительность, методики испытаний (или используются типовые методики), определяются количественный и профессиональный состав аттестационной комиссии, назначаемой органом по аттестации объектов информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации или привлечения испытательных центров (лабораторий) по сертификации средств защиты информации по требованиям безопасности информации.

3.5.2. Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации.

3.5.3. Программа аттестационных испытаний согласовывается с заявителем.

3.6. Заключение договоров на аттестацию

3.6.1. Этап подготовки завершается заключением договора между заявителем и органом по аттестации на проведение аттестации, заключением договоров (контрактов) органа по аттестации с привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.

3.6.2. Оплата работы членов аттестационной комиссии производится органом по аттестации в соответствии с заключенными трудовыми договорами (контрактами) за счет финансовых средств от заключаемых договоров на аттестацию объектов информатизации.

3.7. Проведение аттестационных испытаний объектов информатизации

3.7.1. На этапе аттестационных испытаний объекта информатизации:

- осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;

- определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;

- проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;

- проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

- проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

- оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

3.7.2. Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи "Аттестата соответствия" и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя.

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протоколы испытаний подписываются экспертами - членами аттестационной комиссии, проводившими испытания.

Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

3.8. Оформление, регистрация и выдача "Аттестата соответствия"

3.8.1. "Аттестат соответствия" на объект информатизации, отвечающий требованиям по безопасности информации, выдается органом по аттестации по форме, приведенной в приложении 2.

3.8.2. "Аттестат соответствия" оформляется и выдается заявителю после утверждения заключения по результатам аттестации.

3.8.3. Регистрация "Аттестатов соответствия" осуществляется по отраслевому или территориальному признакам органами по аттестации с целью ведения информационной базы аттестованных объектов информатизации и планирования мероприятий по контролю и надзору.

Ведение сводных информационных баз аттестованных объектов информатизации осуществляется Гостехкомиссией России или по ее поручению одним из органов надзора за аттестацией и эксплуатацией аттестованных объектов.

3.8.4. "Аттестат соответствия" выдается владельцу аттестованного объекта информатизации органом по аттестации на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

3.8.5. В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

3.8.6. При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки орган по аттестации принимает решение об отказе в выдаче "Аттестата соответствия".

При этом может быть предложен срок повторной аттестации при условии устранения недостатков.

При наличии замечаний непринципиального характера "Аттестат соответствия" может быть выдан после проверки устранения этих замечаний.

3.9. Рассмотрение апелляций

В случае несогласия заявителя с отказом в выдаче "Аттестата соответствия" он имеет право обратиться в вышестоящий орган по аттестации или непосредственно в Гостехкомиссию России с апелляцией для дополнительного рассмотрения полученных при испытаниях результатов, где она в месячный срок рассматривается с привлечением заинтересованных сторон. Податель апелляции извещается о принятом решении.

3.10. Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации

3.10.1. Государственный контроль и надзор, инспекционный контроль за проведением аттестации объектов информатизации проводится Гостехкомиссией России как в процессе, так и по завершении аттестации, а за эксплуатацией аттестованных объектов информатизации - периодически в соответствии с планами работы по контролю и надзору.

Гостехкомиссия России может передавать некоторые из своих функций государственного контроля и надзора по аттестации и за эксплуатацией аттестованных объектов информатизации аккредитованным органам по аттестации.

3.10.2. Объем, содержание и порядок государственного контроля и надзора устанавливаются в нормативной и методической документации по аттестации объектов информатизации.

3.10.3. Государственный контроль и надзор за соблюдением правил аттестации включает проверку правильности и полноты проводимых мероприятий по аттестации объектов информатизации, оформления и рассмотрения органами по аттестации отчетных документов и протоколов испытаний, своевременное внесение изменений в нормативную и методическую документацию по безопасности информации, инспекционный контроль за эксплуатацией аттестованных объектов информатизации.

3.10.4. В случае грубых нарушений органом по аттестации требований стандартов или иных нормативных и методических документов по безопасности информации, выявленных при контроле и надзоре, орган по аттестации может быть лишен лицензии на право проведения аттестации объектов информатизации.

3.10.5. При выявлении нарушения правил эксплуатации аттестованных объектов информатизации, технологии обработки защищаемой информации и требований по безопасности информации органом, проводящим контроль и надзор, может быть приостановлено или аннулировано действие "Аттестата соответствия", с оформлением этого решения в "Аттестате соответствия" и информированием органа, ведущего сводную информационную базу аттестованных объектов информатики, и Гостехкомиссии России.

Решение об аннулировании действия "Аттестата соответствия" принимается в случае, когда в результате оперативного принятия организационно-технических мер защиты не может быть восстановлен требуемый уровень безопасности информации.

3.10.6. В случае грубых нарушений органом по аттестации требований стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России, выявленных при контроле и надзоре и приведших к повторной аттестации, расходы по осуществлению контроля и надзора могут быть по решению Госарбитража взысканы с органа по аттестации. Повторная аттестация может быть также осуществлена за счет этого органа по аттестации.

3.10.7. Расходы по осуществлению надзора за обязательной аттестацией и эксплуатацией объектов, прошедших обязательную аттестацию, оплачиваются органом надзора из средств госбюджета, выделенных ему в этих целях.

3.3.3 Результаты и выводы:

Студенты изучили аттестацию объектов информатизации по требованиям безопасности информации.

3.4 Практическое занятие № 5 (2 часа).

Тема: «Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне"»

3.4.1 Задание для работы:

1. Общие положения.
2. Перечень сведений, составляющих государственную тайну.
3. Отнесение сведений к государственной тайне и их засекречивание.

…….

3.4.2 Краткое описание проводимого занятия:

1. Общие положения.

Статья 1. Сфера действия настоящего Закона

Положения настоящего Закона обязательны для исполнения на территории Российской Федерации и за ее пределами органами законодательной, исполнительной и судебной власти, а также организациями, наделенными в соответствии с федеральным законом полномочиями осуществлять от имени Российской Федерации государственное управление в установленной сфере деятельности (далее - органы государственной власти), органами местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.
(в ред. Федеральных законов от 06.10.1997 N 131-ФЗ, от 01.12.2007 N 318-ФЗ)

Статья 2. Основные понятия, используемые в настоящем Законе

В настоящем Законе используются следующие основные понятия:

государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

носители сведений, составляющих государственную тайну, - материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

система защиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;

доступ к сведениям, составляющим государственную тайну, - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Перечень сведений, составляющих государственную тайну, - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

(абзац введен Федеральным законом от 06.10.1997 N 131-ФЗ)

Статья 3. Законодательство Российской Федерации о государственной тайне

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации "О безопасности" и включает настоящий Закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

Статья 4. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты

1. Палаты Федерального Собрания:

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

осуществляют законодательное регулирование отношений в области государственной тайны;

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

абзац исключен. - Федеральный закон от 06.10.1997 N 131-ФЗ;

определяют полномочия должностных лиц в аппаратах палат Федерального Собрания по обеспечению защиты государственной тайны в палатах Федерального Собрания;

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

абзац исключен. - Федеральный закон от 06.10.1997 N 131-ФЗ.

2. Президент Российской Федерации:

утверждает государственные программы в области защиты государственной тайны;

утверждает по представлению Правительства Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;

утверждает по представлению Правительства Российской Федерации Перечень должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне, Перечень должностей, при замещении которых лица считаются допущенными к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;

(в ред. Федерального закона от 18.07.2009 N 180-ФЗ)

заключает международные договоры Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну;

определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента Российской Федерации;

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

3. Правительство Российской Федерации:

организует исполнение Закона Российской Федерации "О государственной тайне";

представляет на утверждение Президенту Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;

представляет на утверждение Президенту Российской Федерации Перечень должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне, Перечень должностей, при замещении которых лица считаются допущенными к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;

(в ред. Федерального закона от 18.07.2009 N 180-ФЗ)

устанавливает порядок разработки Перечня сведений, отнесенных к государственной тайне;

организует разработку и выполнение государственных программ в области защиты государственной тайны;

определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства Российской Федерации;

устанавливает порядок предоставления социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны, если социальные гарантии либо порядок предоставления таких социальных гарантий не установлены федеральными законами или нормативными правовыми актами Президента Российской Федерации;

(в ред. Федеральных законов от 22.08.2004 N 122-ФЗ, от 08.11.2011 N 309-ФЗ)

устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;

заключает межправительственные соглашения, принимает меры по выполнению международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам или международным организациям;

(в ред. Федерального закона от 01.12.2007 N 294-ФЗ)

в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

(абзац введен Федеральным законом от 06.10.1997 N 131-ФЗ)

4. Органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:

обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;

обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства Российской Федерации;

устанавливают размеры предоставляемых социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны на подведомственных им предприятиях, в учреждениях и организациях;

обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;

реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению социальных гарантий лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;

вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.

(п. 4 в ред. Федерального закона от 22.08.2004 N 122-ФЗ)

5. Органы судебной власти:

рассматривают уголовные, гражданские и административные дела о нарушениях законодательства Российской Федерации о государственной тайне;

(в ред. Федерального закона от 08.03.2015 N 23-ФЗ)

обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны;

обеспечивают в ходе рассмотрения указанных дел защиту государственной тайны;

определяют полномочия должностных лиц по обеспечению защиты государственной тайны в органах судебной власти.

2. Перечень сведений, составляющих государственную тайну.

Статья 5. Перечень сведений, составляющих государственную тайну

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Государственную тайну составляют:

1) сведения в военной области:

о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

(в ред. Федерального закона от 11.11.2003 N 153-ФЗ)

3) сведения в области внешней политики и экономики:

о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или

денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты:

(в ред. Федеральных законов от 15.11.2010 N 299-ФЗ, от 21.12.2013 N 377-ФЗ)

о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной, оперативно-розыскной деятельности и деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

(в ред. Федерального закона от 15.11.2010 N 299-ФЗ)

о силах, средствах, об источниках, о методах, планах и результатах деятельности по обеспечению безопасности лиц, в отношении которых принято решение о применении мер государственной защиты, данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения, а также отдельные сведения об указанных лицах;

(абзац введен Федеральным законом от 21.12.2013 N 377-ФЗ)

о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

о методах и средствах защиты секретной информации;

об организации и о фактическом состоянии защиты государственной тайны;

о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;

о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства;

о мерах по обеспечению защищенности критически важных объектов и потенциально опасных объектов инфраструктуры Российской Федерации от террористических актов;

(абзац введен Федеральным законом от 15.11.2010 N 299-ФЗ)

о результатах финансового мониторинга в отношении организаций и физических лиц, полученных в связи с проверкой их возможной причастности к террористической деятельности.
(абзац введен Федеральным законом от 15.11.2010 N 299-ФЗ)

3. Отнесение сведений к государственной тайне и их засекречивание.

Статья 6. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений
(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Отнесение сведений к государственной тайне и их засекречивание - введение в предусмотренном настоящим Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.
(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами законности, обоснованности и своевременности.
(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 настоящего Закона и законодательству Российской Федерации о государственной тайне.
(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Обоснованность отнесения сведений к государственной тайне и их засекречивание заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.
(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Своевременность отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.
(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Статья 7. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию
(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Не подлежат отнесению к государственной тайне и засекречиванию сведения:
(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

(в ред. Федерального закона от 22.08.2004 N 122-ФЗ)

о фактах нарушения прав и свобод человека и гражданина;

о размерах золотого запаса и государственных валютных резервах Российской Федерации;

о состоянии здоровья высших должностных лиц Российской Федерации;

о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суд.

Статья 8. Степени секретности сведений и грифы секретности носителей этих сведений

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "особой важности", "совершенно секретно" и "секретно".

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Статья 9. Порядок отнесения сведений к государственной тайне

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с настоящим Законом.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы

государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым настоящим Законом, руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом Российской Федерации. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, Перечень сведений, отнесенных к государственной тайне. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом Российской Федерации, подлежит открытому опубликованию и пересматривается по мере необходимости.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые перечни сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности. В рамках целевых программ по разработке и модернизации образцов вооружения и военной техники, опытно-конструкторских и научно-исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться отдельные перечни сведений, подлежащих засекречиванию. Эти перечни утверждаются соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.

(в ред. Федерального закона от 06.10.1997 N 131-ФЗ)

Статья 10. Ограничение прав собственности предприятий, учреждений, организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием

Должностные лица, наделенные в порядке, предусмотренном статьей 9 настоящего Закона, полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан (далее - собственник информации), если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных

к государственной тайне. Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.

Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником. В договоре также предусматриваются обязательства собственника информации по ее нераспространению. При отказе собственника информации от подписанного договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну, в соответствии с действующим законодательством.

Собственник информации вправе обжаловать в суд действия должностных лиц, ущемляющие, по мнению собственника информации, его права. В случае признания судом действий должностных лиц незаконными порядок возмещения ущерба, нанесенного собственнику информации, определяется решением суда в соответствии с действующим законодательством.

Не может быть ограничено право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства Российской Федерации.

Статья 11. Порядок засекречивания сведений и их носителей

Основанием для засекречивания сведений, полученных (разработанных) в результате управленческой, производственной, научной и иных видов деятельности органов государственной власти, предприятий, учреждений и организаций, является их соответствие действующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию. При засекречивании этих сведений их носителям присваивается соответствующий гриф секретности.

При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные лица органов государственной власти, предприятий, учреждений и организаций обязаны обеспечить предварительное засекречивание полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направить в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

Должностные лица, утвердившие действующий перечень, обязаны в течение трех месяцев организовать экспертную оценку поступивших предложений и принять решение по дополнению (изменению) действующего перечня или снятию предварительно присвоенного сведениям грифа секретности.

Статья 12. Реквизиты носителей сведений, составляющих государственную тайну

На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;

об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

о регистрационном номере;

о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, эти данные указываются в сопроводительной документации на этот носитель.

Если носитель содержит составные части с различными степенями секретности, каждой из этих составных частей присваивается соответствующий гриф секретности, а носителю в целом присваивается гриф секретности, соответствующий тому грифу секретности, который присваивается его составной части, имеющей высшую для данного носителя степень секретности сведений.

Помимо перечисленных в настоящей статье реквизитов на носителе и (или) в сопроводительной документации к нему могут проставляться дополнительные отметки, определяющие полномочия должностных лиц по ознакомлению с содержащимися в этом носителе сведениями. Вид и порядок проставления дополнительных отметок и других реквизитов определяются нормативными документами, утверждаемыми Правительством Российской Федерации.

3.4.3 Результаты и выводы:

Студенты изучили Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне"

3.5 Практическое занятие № 6 (2 часа).

Тема: «Организационно-технические меры защиты сведений, составляющих государственную тайну, обрабатываемых в автоматизированных информационных системах»

3.5.1 Задание для работы:

1. Организационно-технические меры защиты сведений, составляющих государственную тайну, обрабатываемых в автоматизированных информационных системах.

…….

3.5.2 Краткое описание проводимого занятия:

1. Организационно-технические меры защиты сведений, составляющих государственную тайну, обрабатываемых в автоматизированных информационных системах.

5.1.1. Система (подсистема) защиты информации, обрабатываемой в автоматизированных системах различного уровня и назначения, должна предусматривать комплекс организационных, программных, технических и, при необходимости, криптографических средств и мер по защите информации при ее автоматизированной обработке и хранении, при ее передаче по каналам связи.

5.1.2. Основными направлениями защиты информации являются:

обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения и подделки за счет НСД и специальных воздействий;

обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

5.1.3. В качестве основных мер защиты информации рекомендуются:

документальное оформление перечня сведений конфиденциального характера с учетом ведомственной и отраслевой специфики этих сведений;

реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам, документам;

ограничение доступа персонала и посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации;

разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

регистрация действий пользователей АС и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;

учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение;

использование СЗЗ, создаваемых на основе физико-химических технологий для контроля доступа к объектам защиты и для защиты документов от подделки;

необходимое резервирование технических средств и дублирование массивов и носителей информации;

использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;

использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;

использование сертифицированных средств защиты информации;

размещение объектов защиты на максимально возможном расстоянии относительно границы КЗ;

размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах КЗ;

развязка цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

электромагнитная развязка между линиями связи и другими цепями ВТСС, выходящими за пределы КЗ, и информационными цепями, по которым циркулирует защищаемая информация;
использование защищенных каналов связи (защищенных ВОЛС и криптографических средств ЗИ;
размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр информации;
организация физической защиты помещений и собственно технических средств с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающих нахождение внутри контролируемой зоны технических средств разведки или промышленного шпионажа;
криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи (при необходимости, определяемой особенностями функционирования конкретных АС и систем связи);
предотвращение внедрения в автоматизированные системы программ-вирусов, программных закладок.
Обязательность тех или иных мер для защиты различных видов конфиденциальной информации конкретизирована в последующих подразделах документа.
5.1.4. В целях дифференцированного подхода к защите информации, обрабатываемой в АС различного уровня и назначения, осуществляемого в целях разработки и применения необходимых и достаточных мер и средств защиты информации, проводится классификация автоматизированных систем (форма акта классификации АС приведена в приложении № 1).
5.1.5. Классифицируются АС любого уровня и назначения. Классификация АС осуществляется на основании требований РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" и настоящего раздела документа.
5.1.6. Классификации подлежат все действующие, но ранее не классифицированные, и разрабатываемые АС, предназначенные для обработки конфиденциальной информации.
5.1.7. Если АС, классифицированная ранее, включается в состав вычислительной сети или системы и соединяется с другими техническими средствами линиями связи различной физической природы, образуемая при этом АС более высокого уровня классифицируется в целом, а в отношении АС нижнего уровня классификация не производится.
Если объединяются АС различных классов защищенности, то интегрированная АС должна классифицироваться по высшему классу защищенности входящих в нее АС, за исключением случаев их объединения посредством межсетевого экрана, когда каждая из объединяющихся АС может сохранять свой класс защищенности. Требования к используемым при этом межсетевым экранам изложены в подразделе 5.9.
5.1.8. При рассмотрении и определении режима обработки данных в АС учитывается, что индивидуальным (монопольным) режимом обработки считается режим, при котором ко всей обрабатываемой информации, к программным средствам и носителям информации этой системы допущен только один пользователь.
Режим, при котором различные пользователи, в т.ч. обслуживающий персонал и программисты, работают в одной АС, рассматривается как коллективный. Коллективным режимом работы считается также и последовательный во времени режим работы различных пользователей и обслуживающего персонала.
5.1.9. В случае, когда признаки классифицируемой АС (п. 1.7. РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации") не

совпадают с предложенными в РД (п. 1.9) группами по особенностям обработки информации в АС, то при классификации выбирается наиболее близкая группа защищенности с предъявлением к АС соответствующих дополнительных требований по защите информации. (Например, однопользовательская АС с информацией различного уровня конфиденциальности по формальным признакам не может быть отнесена к 3 группе защищенности. Однако, если дополнительно реализовать в такой системе управление потоками информации, то необходимый уровень защиты будет обеспечен).

5.1.10. Конкретные требования по защите информации и мероприятия по их выполнению определяются в зависимости от установленного для АС класса защищенности. Рекомендуемые классы защищенности АС, СЗЗ, средств защиты информации по уровню контроля отсутствия недекларированных возможностей, а также показатели по классам защищенности СВТ и МЭ от несанкционированного доступа к информации приведены в приложении № 7.

5.1.11. Лица, допущенные к автоматизированной обработке конфиденциальной информации, несут ответственность за соблюдение ими установленного в учреждении (на предприятии) порядка обеспечения защиты этой информации.

Для получения доступа к конфиденциальной информации они должны изучить требования настоящего документа, других нормативных документов по защите информации, действующих в учреждении (на предприятии) в части их касающейся.

5.2. Основные требования и рекомендации по защите служебной тайны и персональных данных

При разработке и эксплуатации АС, предполагающих использование информации, составляющей служебную тайну, а также персональных данных должны выполняться следующие основные требования.

5.2.1. Организация, состав и содержание проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны отвечать требованиям раздела 3.

5.2.2. В учреждении (на предприятии) должны быть документально оформлены перечни сведений, составляющих служебную тайну, и персональных данных, подлежащих защите. Эти перечни могут носить как обобщающий характер в области деятельности учреждения (предприятия), так и иметь отношение к какому-либо отдельному направлению работ. Все исполнители должны быть ознакомлены с этими перечнями в части их касающейся.

5.2.3. В соответствии с РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" устанавливается следующий порядок классификации АС в зависимости от вида сведений конфиденциального характера:

АС, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г;

АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д.

5.2.4. Для обработки информации, составляющей служебную тайну, а также для обработки персональных данных следует использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.

5.2.5. Для передачи информации по каналам связи, выходящим за пределы КЗ, необходимо использовать защищенные каналы связи, в том числе защищенные

волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации. Применяемые средства защиты информации должны быть сертифицированы.
5.2.6. Носители информации на магнитной (магнитно-оптической) и бумажной основе должны учитываться, храниться и уничтожаться в подразделениях учреждений (предприятий) в порядке, установленном для служебной информации ограниченного распространения, с пометкой "Для служебного пользования".
5.2.7. Доступ к информации исполнителей (пользователей, обслуживающего персонала) осуществляется в соответствии с разрешительной системой допуска исполнителей к документам и сведениям конфиденциального характера, действующей в учреждении (на предприятии).
5.2.8. При необходимости указанный минимальный набор рекомендуемых организационно-технических мер защиты информации по решению руководителя предприятия может быть расширен.

5.3. Основные рекомендации по защите информации, составляющей коммерческую тайну

При разработке и эксплуатации АС, предполагающих использование сведений, составляющих коммерческую тайну, рекомендуется выполнение следующих основных организационно-технических мероприятий:
5.3.1. На предприятии следует документально оформить "Перечень сведений, составляющих коммерческую тайну". Все исполнители должны быть ознакомлены с этим "Перечнем".
5.3.2. При организации разработки и эксплуатации АС с использованием таких сведений следует ориентироваться на порядок, приведенный в разделе 3. Оформить порядок разработки и эксплуатации таких АС документально.
5.3.3. Рекомендуется относить АС, обрабатывающие информацию, составляющую коммерческую тайну, режим защиты которой определяет ее собственник, по уровню защищенности к классам 3Б, 2Б и не ниже 1Д (если по решению руководителя предприятия не предъявляются более высокие требования).
5.3.4. Рекомендуется для обработки информации, составляющей коммерческую тайну, использовать средства вычислительной техники, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).
Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.
5.3.5. Для передачи информации по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации.
5.3.6. Следует установить на предприятии порядок учета, хранения и уничтожения носителей информации на магнитной (магнитно-оптической) и бумажной основе в научных, производственных и функциональных подразделениях, а также разработать и ввести в действие разрешительную систему допуска исполнителей документам и сведениям, составляющим коммерческую тайну.
Указанный минимальный набор рекомендуемых организационно-технических мероприятий по решению руководителя предприятия может быть расширен.
Решение о составе и содержании мероприятий, а также используемых средств защиты информации принимается руководителем предприятия по результатам обследования

создаваемой (модернизируемой) АС с учетом важности (ценности) защищаемой информации.

5.4. Порядок обеспечения защиты конфиденциальной информации при эксплуатации АС

5.4.1. Организация эксплуатации АС и СЗИ в ее составе осуществляется в соответствии с установленным в учреждении (на предприятии) порядком, в том числе технологическими инструкциями по эксплуатации СЗИ НСД для пользователей, администраторов АС и работников службы безопасности.

5.4.2. Для обеспечения защиты информации в процессе эксплуатации АС рекомендуется предусматривать соблюдение следующих основных положений и требований:

допуск к защищаемой информации лиц, работающих в АС (пользователей, обслуживающего персонала), должен производиться в соответствии с установленным разрешительной системой допуска порядком;

на период обработки защищаемой информации в помещениях, где размещаются ОТСС, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации; допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в эти помещения только с санкции руководителя учреждения (предприятия) или руководителя службы безопасности;

в случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации;

по окончании обработки защищаемой информации или при передаче управления другому лицу пользователь обязан произвести стирание временных файлов на несъёмных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ПЭВМ;

изменение или ввод новых программ обработки защищаемой информации в АС должен осуществляться совместно разработчиком АС и администратором АС;

при увольнении или перемещении администраторов АС руководителем учреждения (предприятия) по согласованию со службой безопасности должны быть приняты меры по оперативному изменению паролей, идентификаторов и ключей шифрования.

5.4.3. Все носители информации на бумажной, магнитной, оптической (магнито-оптической) основе, используемые в технологическом процессе обработки информации в АС, подлежат учету в том производственном, научном или функциональном подразделении, которое является владельцем АС, обрабатывающей эту информацию.

5.4.4. Учет съемных носителей информации на магнитной или оптической основе (гибкие магнитные диски, съемные накопители информации большой емкости или картриджи, съемные пакеты дисков, иные магнитные, оптические или магнито-оптические диски, магнитные ленты и т.п.), а также распечаток текстовой, графической и иной информации на бумажной или пластиковой (прозрачной) основе осуществляется по карточкам или журналам установленной формы, в том числе автоматизировано с использованием средств вычислительной техники. Журнальная форма учета может использоваться в АС с небольшим объемом документооборота.

5.4.5. Съемные носители информации на магнитной или оптической основе в зависимости от характера или длительности использования допускается учитывать совместно с другими документами по установленным для этого учетным формам.

При этом перед выполнением работ сотрудником, ответственным за их учет, на этих носителях информации предварительно проставляются любым доступным способом следующие учетные реквизиты: учетный номер и дата, пометка "Для служебного пользования", номер экземпляра, подпись этого сотрудника, а также другие возможные реквизиты, идентифицирующие этот носитель.

5.4.6. Распечатки допускается учитывать совместно с другими традиционными печатными документами по установленным для этого учетным формам.
5.4.7. Временно не используемые носители информации должны храниться пользователем в местах, недоступных для посторонних лиц.

5.5. Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ

5.5.1. Автоматизированные рабочие места на базе автономных ПЭВМ являются автоматизированными системами, обладающими всеми основными признаками АС. Информационным каналом обмена между такими АС являются носители информации на магнитной (магнитно-оптической) и бумажной основе.
В связи с этим порядок разработки и эксплуатации АРМ на базе автономных ПЭВМ по составу и содержанию проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны полностью отвечать требованиям настоящего документа.
5.5.2. АС на базе автономных ПЭВМ в соответствии с требованиями РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" должны быть классифицированы и отнесены:
к 3 группе АС, если в ней работает только один пользователь, допущенный ко всей информации АС;
ко 2 и 1 группе АС, если в ней последовательно работают несколько пользователей с равными или разными правами доступа (полномочиями), соответственно.
Примечание: При использовании на автономной ПЭВМ технологии обработки информации на съемных накопителях большой емкости, классификация АС производится на основании анализа режима доступа пользователей АС к информации на используемом съемном накопителе (либо одновременно используемом их комплексе).

5.6. Защита информации при использовании съемных накопителей информации большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ

5.6.1. Данная информационная технология предусматривает запись на загружаемый съемный накопитель информации большой емкости одновременно общесистемного (ОС, СУБД) и прикладного программного обеспечения, а также обрабатываемой информации одного или группы пользователей.
В качестве устройств для работы по этой технологии могут быть использованы накопители на магнитном, магнито-оптическом или лазерном дисках различной конструкции, как встроенные (съемные), так и выносные. Одновременно может быть установлено несколько съемных накопителей информации большой емкости.
Несъемные накопители должны быть исключены из конфигурации ПЭВМ.
Основной особенностью применения данной информационной технологии для АРМ на базе автономных ПЭВМ с точки зрения защиты информации является исключение этапа хранения на ПЭВМ в нерабочее время информации, подлежащей защите.
Эта особенность может быть использована для обработки защищаемой информации без применения сертифицированных средств защиты информации от НСД и использования средств физической защиты помещений этих АРМ.
5.6.2. На этапе предпроектного обследования необходимо провести детальный анализ технологического процесса обработки информации, обращая внимание, прежде всего, на технологию обмена информацией (при использовании съемных накопителей информации большой емкости или гибких магнитных дисков (ГМД или дискет) с другими АРМ, как использующими, так и не использующими эту информационную технологию, на создание условий, исключающих попадание конфиденциальной информации на неучтенные

носители информации, несанкционированное ознакомление с этой информацией, на организацию выдачи информации на печать.
5.6.3. Обмен конфиденциальной информацией между АРМ должен осуществляться только на учтенных носителях информации с учетом допуска исполнителей, работающих на АРМ, к переносимой информации.
5.6.4. На рабочих местах исполнителей, работающих по этой технологии, во время работы, как правило, не должно быть неучтенных накопителей информации.
В случае формирования конфиденциальных документов с использованием, как текстовой, так и графической информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть "закрыты на запись".
Условия и порядок применения таких процедур должны быть отражены в технологии обработки информации, использующей съемные накопители информации большой емкости.
5.6.5. При использовании в этой технологии современных средств вычислительной техники, оснащенных энергонезависимой, управляемой извне перезаписываемой памятью, так называемых Flash-Bios (FB), необходимо обеспечить целостность записанной в FB информации. Для обеспечения целостности, как перед началом работ, с конфиденциальной информацией при загрузке ПЭВМ, так и по их окончании, необходимо выполнить процедуру проверки целостности FB. При несовпадении необходимо восстановить (записать первоначальную версию) FB, поставить об этом в известность руководителя подразделения и службу безопасности, а также выяснить причины изменения FB.
5.6.6. Должна быть разработана и по согласованию с службой безопасности утверждена руководителем учреждения (предприятия) технология обработки конфиденциальной информации, использующая съемные накопители информации большой емкости и предусматривающая вышеуказанные, а также другие вопросы защиты информации, имеющие отношение к условиям размещения, эксплуатации АРМ, учету носителей информации, а также другие требования, вытекающие из особенностей функционирования АРМ.

5.7. Защита информации в локальных вычислительных сетях

5.7.1. Характерными особенностями ЛВС являются распределенное хранение файлов, удаленная обработка данных (вычисления) и передача сообщений (электронная почта), а также сложность проведения контроля за работой пользователей и состоянием общей безопасности ЛВС.
5.7.2. Средства защиты информации от НСД должны использоваться во всех узлах ЛВС независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС и требуют постоянного квалифицированного сопровождения со стороны администратора безопасности информации.
5.7.3. Информация, составляющая служебную тайну, и персональные данные могут обрабатываться только в изолированных ЛВС, расположенных в пределах контролируемой зоны, или в условиях, изложенных в пунктах 5.8.4. и 5.8.5. следующего подраздела.
5.7.4. Класс защищенности ЛВС определяется в соответствии с требованиями РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации".
5.7.5. Для управления ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, в дополнение к системным администраторам (администраторам ЛВС) могут быть

назначены администраторы по безопасности информации, имеющие необходимые привилегии доступа к защищаемой информации ЛВС.
5.7.6. Состав пользователей ЛВС должен устанавливаться по письменному разрешению руководства предприятия (структурного подразделения) и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.
5.7.7. Каждый администратор и пользователь должен иметь уникальные идентификаторы и пароли, а в случае использования криптографических средств защиты информации - ключи шифрования для криптографических средств, используемых для защиты информации при передаче ее по каналам связи и хранения, и для систем электронной цифровой подписи.

5.8. Защита информации при межсетевом взаимодействии

5.8.1. Положения данного подраздела относятся к взаимодействию локальных сетей, ни одна из которых не имеет выхода в сети общего пользования типа Internet.
5.8.2. Взаимодействие ЛВС с другими вычислительными сетями должно контролироваться с точки зрения защиты информации. Коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах КЗ.
5.8.3. При конфигурировании коммуникационного оборудования (маршрутизаторов, концентраторов, мостов и мультиплексоров) и прокладке кабельной системы ЛВС рекомендуется учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия.
5.8.4. Подключение ЛВС к другой автоматизированной системе (локальной или неоднородной вычислительной сети) иного класса защищенности должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".
5.8.5. Для защиты конфиденциальной информации при ее передаче по каналам связи из одной АС в другую необходимо использовать:
в АС класса 1Г - МЭ не ниже класса 4;
в АС класса 1Д и 2Б, 3Б - МЭ класса 5 или выше.
Если каналы связи выходят за пределы КЗ, необходимо использовать защищенные каналы связи, защищенные волоконно-оптические линии связи либо сертифицированные криптографические средства защиты.

5.9. Защита информации при работе с системами управления базами данных

5.9.1. При работе с системами управления базами данных (СУБД) и базами данных (БД) необходимо учитывать следующие особенности защиты информации от НСД:
в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;
БД могут быть физически распределены по различным устройствам и узлам сети;
БД могут включать информацию различного уровня конфиденциальности;
разграничение доступа пользователей к БД средствами операционной системы и/или СЗИ НСД может осуществляться только на уровне файлов БД;
разграничение доступа пользователей к объектам БД: таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п., может осуществляться только средствами СУБД, если таковые имеются;
регистрация действий пользователей при работе с объектами БД может осуществляться также только средствами СУБД, если таковые имеются;

СУБД могут обеспечивать одновременный доступ многих пользователей (клиентов) к БД с помощью сетевых протоколов, при этом запросы пользователя к БД обрабатываются на сервере и результаты обработки направляются пользователям (клиентам).
5.9.2. С учетом указанных особенностей при создании БД рекомендуется:
при выборе СУБД ориентироваться на операционные системы и СУБД, включающие либо штатные сертифицированные средства защиты информации от НСД, либо имеющие соответствующие сертифицированные дополнения в виде СЗИ НСД;
при использовании СУБД, не имеющих средств разграничения доступа, производить разбиение БД на отдельные файлы, разграничение доступа к которым можно проводить средствами ОС и/или СЗИ НСД;
при использовании современных СУБД, основанных на модели клиент-сервер, использовать их штатные средства защиты информации от НСД, применять средства регистрации (аудита) и разграничение доступа к объектам БД на основе прав, привилегий, ролей, представлений (VIEW), процедур и т.п.

3.5.3 Результаты и выводы:

Студенты изучили организационно-технические меры защиты сведений, составляющих государственную тайну, обрабатываемых в автоматизированных информационных системах.

3.6 Практическое занятие № 7 (2 часа).

Тема: «Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации»

3.6.1 Задание для работы:

1. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.
2. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации.
3. Государственное регулирование в сфере применения информационных технологий.

…….

3.6.2 Краткое описание проводимого занятия:

1. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

2. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Статья 5. Информация как объект правовых отношений

1. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения

доступа к информации либо иные требования к порядку ее предоставления или распространения.

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Статья 6. Обладатель информации

1. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

3. Государственное регулирование в сфере применения информационных технологий.

Статья 12. Государственное регулирование в сфере применения информационных технологий

1. Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей;

4) обеспечение информационной безопасности детей.

(п. 4 введен Федеральным законом от 21.07.2011 N 252-ФЗ)

2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Статья 12.1. Особенности государственного регулирования в сфере использования российских программ для электронных вычислительных машин и баз данных

(введена Федеральным законом от 29.06.2015 N 188-ФЗ)

1. В целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки создается единый реестр российских программ для электронных вычислительных машин и баз данных (далее - реестр российского программного обеспечения).

2. Правила формирования и ведения реестра российского программного обеспечения, состав сведений, включаемых в реестр российского программного обеспечения, в том числе об основаниях возникновения исключительного права у правообладателя (правообладателей), условия включения таких сведений в реестр российского программного обеспечения и исключения их из реестра российского программного обеспечения, порядок предоставления сведений, включаемых в реестр российского программного обеспечения, порядок принятия решения о включении таких сведений в реестр российского программного обеспечения устанавливаются Правительством Российской Федерации.

3. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра российского программного обеспечения оператора реестра российского программного обеспечения - организацию, зарегистрированную на территории Российской Федерации.

4. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти утверждает классификатор программ для электронных вычислительных машин и баз данных в целях ведения реестра российского программного обеспечения.

5. В реестр российского программного обеспечения включаются сведения о программах для электронных вычислительных машин и базах данных, которые соответствуют следующим требованиям:

1) исключительное право на программу для электронных вычислительных машин или базу данных на территории всего мира и на весь срок действия исключительного права принадлежит одному либо нескольким из следующих лиц (правообладателей):

а) Российской Федерации, субъекту Российской Федерации, муниципальному образованию;

б) российской некоммерческой организации, высший орган управления которой формируется прямо и (или) косвенно Российской Федерацией, субъектами Российской Федерации, муниципальными образованиями и (или) гражданами Российской Федерации и решения которой иностранное лицо не имеет возможности определять в силу особенностей отношений между таким иностранным лицом и российской некоммерческой организацией;

в) российской коммерческой организации, в которой суммарная доля прямого и (или) косвенного участия Российской Федерации, субъектов Российской Федерации, муниципальных образований, российских некоммерческих организаций, указанных в подпункте "б" настоящего пункта, граждан Российской Федерации составляет более пятидесяти процентов;

г) гражданину Российской Федерации;

2) программа для электронных вычислительных машин или база данных правомерно введена в гражданский оборот на территории Российской Федерации, экземпляры программы для электронных вычислительных машин или базы данных либо права использования программы для электронных вычислительных машин или базы данных свободно реализуются на всей территории Российской Федерации;

3) общая сумма выплат по лицензионным и иным договорам, предусматривающим предоставление прав на результаты интеллектуальной деятельности и средства индивидуализации, выполнение работ, оказание услуг в связи с разработкой, адаптацией и модификацией программы для электронных вычислительных машин или базы данных и для разработки, адаптации и модификации программы для электронных вычислительных машин или базы данных, в пользу иностранных юридических лиц и (или) физических лиц, контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций, агентов, представителей иностранных лиц и контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций составляет менее тридцати процентов от выручки правообладателя (правообладателей) программы для электронных вычислительных машин или базы данных от реализации программы для электронных вычислительных машин или базы данных, включая предоставление прав использования, независимо от вида договора за календарный год;

4) сведения о программе для электронных вычислительных машин или базе данных не составляют государственную тайну, и программа для электронных вычислительных машин или база данных не содержит сведений, составляющих государственную тайну.

6. Правительством Российской Федерации могут быть установлены дополнительные требования к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения.

7. Программы для электронных вычислительных машин и базы данных, сведения о которых включены в реестр российского программного обеспечения, признаются происходящими из Российской Федерации.

8. Для целей настоящей статьи доля участия одной организации в другой организации или гражданина Российской Федерации в организации определяется в соответствии с порядком, установленным главой 14.1 Налогового кодекса Российской Федерации.

9. Для целей настоящей статьи контролируемой иностранным лицом российской коммерческой организацией или российской некоммерческой организацией признается организация, решения которой иностранное лицо имеет возможность определять в силу преобладающего прямого и (или) косвенного участия в этой организации, участия в договоре (соглашении), предметом которого является управление этой организацией, или иных особенностей отношений между иностранным лицом и этой организацией и (или) иными лицами.

10. Решение об отказе во включении в реестр российского программного обеспечения программ для электронных вычислительных машин или баз данных может быть обжаловано правообладателем программы для электронных вычислительных машин или базы данных в суд в течение трех месяцев со дня получения такого решения.

3.6.3 Результаты и выводы:

Студенты изучили Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

3.7 Практическое занятие № 8 (2 часа).

Тема: «Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"»

3.7.1 Задание для работы:

1. Законодательство Российской Федерации о коммерческой тайне.
2. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации.
3. Охрана конфиденциальности информации.

…….

3.7.2 Краткое описание проводимого занятия:

1. Законодательство Российской Федерации о коммерческой тайне.

Статья 1. Цели и сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

(часть 1 в ред. Федерального закона от 12.03.2014 N 35-ФЗ)

2. Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

3. Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Статья 2. Утратила силу с 1 октября 2014 года. - Федеральный закон от 12.03.2014 N 35-ФЗ.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

(п. 1 в ред. Федерального закона от 18.12.2006 N 231-ФЗ)

2) информация, составляющая коммерческую тайну, - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

(п. 2 в ред. Федерального закона от 12.03.2014 N 35-ФЗ)

3) утратил силу с 1 января 2008 года. - Федеральный закон от 18.12.2006 N 231-ФЗ;

4) обладатель информации, составляющей коммерческую тайну, - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

5) доступ к информации, составляющей коммерческую тайну, - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

6) передача информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

7) контрагент - сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

8) предоставление информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

9) разглашение информации, составляющей коммерческую тайну, - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Статья 4. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации

1. Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.

2. Утратил силу с 1 января 2008 года. - Федеральный закон от 18.12.2006 N 231-ФЗ.

3. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

4. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

2. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации.

Статья 4. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации

1. Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.

2. Утратил силу с 1 января 2008 года. - Федеральный закон от 18.12.2006 N 231-ФЗ.

3. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

4. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

Статья 5. Сведения, которые не могут составлять коммерческую тайну

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

3. Охрана конфиденциальности информации.

Статья 10. Охрана конфиденциальности информации

1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

(п. 5 в ред. Федерального закона от 11.07.2011 N 200-ФЗ)

2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.

3. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране конфиденциальности информации, указанные в части 1 настоящей статьи, за исключением пунктов 1 и 2, а также положений пункта 4, касающихся регулирования трудовых отношений.

4. Наряду с мерами, указанными в части 1 настоящей статьи, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Статья 11. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений
(в ред. Федерального закона от 12.03.2014 N 35-ФЗ)

1. В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан:

1) ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

2. Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

3. В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работник обязан:

1) выполнять установленный работодателем режим коммерческой тайны;

2) не разглашать эту информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

3) возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

4) передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну.

4. Работодатель вправе потребовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если эта информация разглашена в течение срока действия режима коммерческой тайны.

5. Причиненные работником или прекратившим трудовые отношения с работодателем лицом убытки не возмещаются, если разглашение информации, составляющей коммерческую тайну, произошло вследствие несоблюдения работодателем мер по обеспечению режима коммерческой тайны, действий третьих лиц или непреодолимой силы.

6. Трудовым договором с руководителем организации должны предусматриваться его обязанности по обеспечению охраны конфиденциальности составляющей коммерческую тайну информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны конфиденциальности этой информации.

7. Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством.

8. Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

3.7.3 Результаты и выводы:

Студенты изучили Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"

3.8 Практическое занятие № 9 (2 часа).

Тема: «Организационно-технические меры защиты коммерческой тайны, обрабатываемой в автоматизированных информационных системах»

3.8.1 Задание для работы:

1. Организационно-технические меры защиты коммерческой тайны, обрабатываемой в автоматизированных информационных системах.

…….

3.8.2 Краткое описание проводимого занятия:

1. Организационно-технические меры защиты коммерческой тайны, обрабатываемой в автоматизированных информационных системах.

2.1. Настоящий документ устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты конфиденциальной информации на территории Российской Федерации и является основным руководящим документом в этой области для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, предприятий, учреждений и организаций (далее - учреждения и предприятия) независимо от их организационно-правовой формы и формы собственности, должностных лиц и граждан Российской Федерации, взявшим на себя обязательства либо обязанными по статусу исполнять требования правовых документов Российской Федерации по защите информации.

2.2. Требования и рекомендации настоящего документа распространяются на защиту:

- конфиденциальной информации - информации с ограниченным доступом, за исключением сведений, отнесенных к государственной тайне и персональным данным,

содержащейся в государственных (муниципальных) информационных ресурсах, накопленной за счет государственного (муниципального) бюджета и являющейся собственностью государства (к ней может быть отнесена информация, составляющая служебную тайну и другие виды тайн в соответствии с законодательством Российской Федерации, а также сведения конфиденциального характера в соответствии с "Перечнем сведений конфиденциального характера", утвержденного Указом Президента Российской Федерации от 06.03.97 №188), защита которой осуществляется в интересах государства (далее - служебная тайна);

- информации о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющей идентифицировать его личность (персональные данные) *(В соответствии с Федеральным законом "Об информации, информатизации и защите информации" режим защиты персональных данных должен быть определен федеральным законом. До его введения в действие для установления режима защиты такой информации следует руководствоваться настоящим документом., за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.)*

2.3. Для защиты конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой определяет собственник этих ресурсов (например, информации, составляющей коммерческую, банковскую тайну и т.д.) (далее - коммерческая тайна), данный документ носит рекомендательный характер.

2.4. Документ разработан на основании федеральных законов "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", Указа Президента Российской Федерации от 06.03.97г. № 188 "Перечень сведений конфиденциального характера", "Доктрины информационной безопасности Российской Федерации", утвержденной Президентом Российской Федерации 09.09.2000г. № Пр.-1895, "Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти", утвержденного постановлением Правительства Российской Федерации от 03.11.94г. № 1233, других нормативных правовых актов по защите информации (приложение № 8), а также опыта реализации мер защиты информации в министерствах и ведомствах, в учреждениях и на предприятиях.

2.5. Документ определяет следующие основные вопросы защиты информации:

- организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;
- состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;
- требования и рекомендации по защите речевой информации при осуществлении переговоров, в том числе с использованием технических средств;
- требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;
- порядок обеспечения защиты информации при эксплуатации объектов информатизации;
- особенности защиты информации при разработке и эксплуатации автоматизированных систем, использующих различные типы средств вычислительной техники и информационные технологии;
- порядок обеспечения защиты информации при взаимодействии абонентов с информационными сетями общего пользования.

Порядок разработки, производства, реализации и использования средств криптографической защиты информации определяется "Положением о порядке

разработки, производства (изготовления), реализации, приобретения и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну" (Положение ПКЗ-99), а также "Инструкцией по организации и обеспечению безопасности хранения, обработки и передачи по техническим каналам связи конфиденциальной информации в Российской Федерации с использованием сертифицированных ФАПСИ криптографических средств".

2.6. Защита информации, обрабатываемой с использованием технических средств, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в установленном настоящим документом порядке в виде системы (подсистемы) защиты информации во взаимосвязи с другими мерами по защите информации.

2.7. Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в АС.

Защищаемыми объектами информатизации являются:

- средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации;
- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);
- защищаемые помещения.

2.8. Защита информации должна осуществляться посредством выполнения комплекса мероприятий и применение (при необходимости) средств ЗИ по предотвращению утечки информации или воздействия на нее по техническим каналам, за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

2.9. При ведении переговоров и использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

- акустическое излучение информативного речевого сигнала;
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы КЗ;
- виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
- несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;

- воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;
- побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;
- наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;
- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом;
- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- прослушивание ведущихся телефонных и радиопереговоров;
- просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

2.10. Перехват информации или воздействие на нее с использованием технических средств могут вестись:

- из-за границы КЗ из близлежащих строений и транспортных средств;
- из смежных помещений, принадлежащих другим учреждениям (предприятиям) и расположенным в том же здании, что и объект защиты;
- при посещении учреждения (предприятия) посторонними лицами;
- за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через информационные сети общего пользования.

2.11. В качестве аппаратуры перехвата или воздействия на информацию и технические средства могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта защиты либо подключаемые к каналам связи или техническим средствам обработки информации, а также электронные устройства перехвата информации "закладки", размещаемые внутри или вне защищаемых помещений.

2.12. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

- непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;
- случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;
- некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;

- просмотра информации с экранов дисплеев и других средств ее отображения.

2.13. Выявление и учет факторов воздействующих или могущих воздействовать на защищаемую информацию (угроз безопасности информации) в конкретных условиях, в соответствии с ГОСТ Р 51275-99, составляют основу для планирования и осуществления мероприятий, направленных на защиту информации на объекте информатизации.

Перечень необходимых мер защиты информации определяется по результатам обследования объекта информатизации с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения санкционированной доступности информации и работоспособности технических средств, обрабатывающих эту информацию, а также с учетом реальных возможностей ее перехвата и раскрытия ее содержания.

2.14. Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности информации реализуются без применения сложных технических средств перехвата информации:

- речевой информации, циркулирующей в защищаемых помещениях;
- информации, обрабатываемой средствами вычислительной техники, от несанкционированного доступа и несанкционированных действий;
- информации, выводимой на экраны видеомониторов;
- информации, передаваемой по каналам связи, выходящим за пределы КЗ.

2.15. Разработка мер и обеспечение защиты информации осуществляются подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководством предприятия (учреждения) для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии Гостехкомиссии России и/или ФАПСИ на право оказания услуг в области защиты информации.

2.16. Для защиты информации рекомендуется использовать сертифицированные по требованиям безопасности информации технические средства обработки и передачи информации, технические и программные средства защиты информации.

При обработке документированной конфиденциальной информации на объектах информатизации в органах государственной власти Российской Федерации и органах государственной власти субъектов Российской Федерации, других государственных органах, предприятиях и учреждениях средства защиты информационных систем подлежат обязательной сертификации.

2.17. Объекты информатизации должны быть аттестованы на соответствие требованиям по защите информации *(Здесь и далее под аттестацией понимается комиссионная приемка объекта информатизации силами предприятия с обязательным участием специалиста по защите информации.)*

2.18. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителей учреждений и предприятий, эксплуатирующих объекты информатизации.

3.8.3 Результаты и выводы:

Студенты изучили организационно-технические меры защиты коммерческой тайны, обрабатываемой в автоматизированных информационных системах.

3.9 Практическое занятие № 10 (2 часа).

Тема: «Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

3.9.1 Задание для работы:

1. Общие положения.
2. Требования к организации защиты информации, содержащейся в информационной системе.
3. Формирование требований к защите информации, содержащейся в информационной системе.

…….

3.9.2 Краткое описание проводимого занятия:

1. Общие положения.

1. Настоящие Требования разработаны в соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328), а также с учетом национальных стандартов Российской Федерации в области защиты информации и в области создания автоматизированных систем (далее – национальные стандарты).

2. В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее – защита информации) при обработке указанной информации в государственных информационных системах.

Настоящие Требования могут применяться для защиты общедоступной информации, содержащейся в государственных информационных системах, для достижения целей, указанных в пунктах 1 и 3 части 1 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации». В документе не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

3. Настоящие Требования являются обязательными при обработке информации в государственных информационных системах, функционирующих на территории Российской Федерации, а также в муниципальных информационных системах, если иное не установлено законодательством Российской Федерации о местном самоуправлении.

Настоящие Требования не распространяются на государственные информационные системы Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, Высшего Арбитражного Суда Российской Федерации и Федеральной службы безопасности Российской Федерации.

4. Настоящие Требования предназначены для обладателей информации, заказчиков, заключивших государственный контракт на создание государственной информационной

системы (далее – заказчики) и операторов государственных информационных систем (далее – операторы).

Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (далее – уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии с настоящими Требованиями.

5. При обработке в государственной информационной системе информации, содержащей персональные данные, настоящие Требования применяются наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

6. По решению обладателя информации (заказчика) или оператора настоящие Требования могут применяться для защиты информации, содержащейся в негосударственных информационных системах.

7. Защита информации, содержащейся в государственной информационной системе (далее – информационная система), обеспечивается путем выполнения обладателем информации (заказчиком) и (или) оператором требований к организации защиты информации, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе.

2. Требования к организации защиты информации, содержащейся в информационной системе.

8. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

9. Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

10. Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности» (Собрание законодательства Российской Федерации, 2011, N 19, ст. 2716; N 30, ст. 4590; N 43, ст. 5971; N 48, ст. 6728; 2012, N 26, ст. 3446; N 31, ст. 4322; 2013, N 9, ст. 874).

11. Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в

соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании» (Собрание законодательства Российской Федерации, 2002, N 52, ст. 5140; 2007, N 19, ст. 2293; N 49, ст. 6070; 2008, N 30, ст. 3616; 2009, N 29, ст. 3626; N 48, ст. 5711; 2010, N 1, ст. 6; 2011, N 30, ст. 4603; N 49, ст. 7025; N 50, ст. 7351; 2012, N 31, ст. 4322; 2012, N 50, ст. 6959).

12. Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее – система защиты информации информационной системы).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:
неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

неправомерного блокирования информации (обеспечение доступности информации).

13. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

разработка системы защиты информации информационной системы;

внедрение системы защиты информации информационной системы;

аттестация информационной системы по требованиям защиты информации (далее –

аттестация информационной системы) и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

3. Формирование требований к защите информации, содержащейся в информационной системе.

14. Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации (заказчиком).

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее - ГОСТ Р 51583) и ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее - ГОСТ Р 51624) и в том числе

включает:
принятие решения о необходимости защиты информации, содержащейся в информационной системе;

классификацию информационной системы по требованиям защиты информации (далее – классификация информационной системы);

определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

определение требований к системе защиты информации информационной системы.

14.1. При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:

анализ целей создания информационной системы и задач, решаемых этой информационной системой;

определение информации, подлежащей обработке в информационной системе;

анализ нормативных правовых актов, методических документов и национальных стандартов,

которым должна соответствовать информационная система;

принятие решения о необходимости создания системы защиты информации информационной системы, а также определение целей и задач защиты информации в информационной системе, основных этапов создания системы защиты информации информационной системы и функций по обеспечению защиты информации, содержащейся в информационной системе, обладателя информации (заказчика), оператора и уполномоченных лиц.

14.2. Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый).

Устанавливаются четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый. Класс защищенности информационной системы определяется в соответствии с приложением N 1 к настоящим Требованиям.

Класс защищенности определяется для информационной системы в целом и, при необходимости, для ее отдельных сегментов (составных частей). Требование к классу защищенности включается в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (далее – ГОСТ 34.602), ГОСТ Р 51583 и ГОСТ Р 51624.
Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Результаты классификации информационной системы оформляются актом классификации.

14.3. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных

способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818).

14.4. Требования к системе защиты информации информационной системы определяются в зависимости от класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации. Требования к системе защиты информации информационной системы включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

цель и задачи обеспечения защиты информации в информационной системе;

класс защищенности информационной системы;

перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

перечень объектов защиты информационной системы;

требования к мерам и средствам защиты информации, применяемым в информационной системе;

требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении

вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

При определении требований к системе защиты информации информационной системы учитываются положения политик обеспечения информационной безопасности обладателя информации (заказчика) в случае их разработки по ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», а также политик обеспечения информационной безопасности оператора и уполномоченного лица в части, не противоречащей политикам обладателя информации (заказчика).

3.9.3 Результаты и выводы:

Студенты изучили защиту информации, не составляющую государственную тайну, содержащуюся в государственных информационных системах.

3.10 Практическое занятие № 11 (2 часа).

Тема: «Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.12.2013) "О персональных данных"»

3.10.1 Задание для работы:

1. Сфера действия настоящего Федерального закона.
2. Принципы и условия обработки персональных данных.
3. Право субъекта персональных данных на доступ к его персональным данным.

…….

3.10.2 Краткое описание проводимого занятия:

1. Сфера действия настоящего Федерального закона.

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

(часть 1 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) утратил силу. - Федеральный закон от 25.07.2011 N 261-ФЗ;

4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

5) предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации".

(п. 5 введен Федеральным законом от 28.06.2010 N 123-ФЗ)

Статья 2. Цель настоящего Федерального закона

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

В целях настоящего Федерального закона используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение,

использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Принципы и условия обработки персональных данных.

Статья 5. Принципы обработки персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Статья 6. Условия обработки персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации

предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
(в ред. Федерального закона от 05.04.2013 N 43-ФЗ)

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
(п. 5 в ред. Федерального закона от 21.12.2013 N 363-ФЗ)

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных,

предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Статья 7. Конфиденциальность персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Статья 8. Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.
(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.
(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Статья 9. Согласие субъекта персональных данных на обработку его персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона, возлагается на оператора.

КонсультантПлюс: примечание.
В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 02.07.2013) в случаях, если федеральными законами и иными нормативными правовыми актами, вступившими в силу до 1 июля 2013 года, предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись.

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

Статья 10. Специальные категории персональных данных

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные сделаны общедоступными субъектом персональных данных;

(п. 2 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

(п. 2.1 введен Федеральным законом от 25.11.2009 N 266-ФЗ)

2.2) обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";

(п. 2.2 введен Федеральным законом от 27.07.2010 N 204-ФЗ)

2.3) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

(п. 2.3 введен Федеральным законом от 25.07.2011 N 261-ФЗ, в ред. Федерального закона от 21.07.2014 N 216-ФЗ)

3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

(п. 3 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

(п. 6 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

(п. 7 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

7.1) обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;
(п. 7.1 введен Федеральным законом от 23.07.2013 N 205-ФЗ)

8) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
(п. 8 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

9) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;
(п. 9 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

10) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.
(п. 10 введен Федеральным законом от 04.06.2014 N 142-ФЗ)

3. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

4. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных частями 2 и 3 настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.
(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Статья 11. Биометрические персональные данные

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о

транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

(в ред. Федерального закона от 04.06.2014 N 142-ФЗ)

Статья 12. Трансграничная передача персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и

безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Статья 13. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных

1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

3. Право субъекта персональных данных на доступ к его персональным данным.

Статья 14. Право субъекта персональных данных на доступ к его персональным данным

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения, указанные в части 7 настоящей статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

КонсультантПлюс: примечание.
В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 02.07.2013) в случаях, если федеральными законами и иными нормативными правовыми актами, вступившими в силу до 1 июля 2013 года, предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись.

3. Сведения, указанные в части 7 настоящей статьи, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. В случае, если сведения, указанные в части 7 настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7

настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 настоящей статьи, должен содержать обоснование направления повторного запроса.

6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

3.10.3 Результаты и выводы:

Студенты изучили Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.12.2013) "О персональных данных"

3.11 Практическое занятие № 12 (2 часа).

Тема: «Требования к защите персональных данных при их обработке в информационных системах персональных данных»

3.11.1 Задание для работы:

1. Общие положения.
2. Типы угроз безопасности персональных данных.
3. Уровни защищенности персональных данных.

…….

3.11.2 Краткое описание проводимого занятия:

1. Общие положения.

1. Настоящий документ разработан в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; 2011, N 23, ст. 3263; N 31, ст. 4701) и устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - меры по обеспечению безопасности персональных данных) для каждого из уровней защищенности персональных данных, установленных в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением

Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В настоящем документе не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

2. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система) обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

3. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда, применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

6. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

7. Меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328).

2. Типы угроз безопасности персональных данных.

8. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к настоящему документу.

8.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

8.2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

8.3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

8.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

8.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

8.6. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

8.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

8.8. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

8.9. Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

8.10. Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

8.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

8.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту

персональных данных, представленных в виде информативных электрических сигналов и физических полей.

8.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

8.14. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

8.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

9. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;

адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

10. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

11. В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, указанным в пункте 8 настоящего документа, могут применяться следующие меры:

проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

тестирование информационной системы на проникновения;

использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

12. При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

а) для обеспечения 1 и 2 уровней защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия информационной системы с информационнотелекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

б) для обеспечения 3 уровня защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

в) для обеспечения 4 уровня защищенности персональных данных применяются: .

средства вычислительной техники не ниже 6 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;

межсетевые экраны 5 класса.

Для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

13. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 настоящего документа.

3. Уровни защищенности персональных данных.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе	+	+	+	+

	внешних пользователей				
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до		+	+	+

	идентификации и аутентификации				
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				

IV. Защита машинных носителей персональных данных (ЗНИ)					
ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ. 2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных,хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в				

	том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ. 7	Защита информации о событиях безопасности	+	+	+	+
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.I	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей,			+	+

	реализации правил разграничения доступа, полномочий пользователей в информационной системе				
IX.Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ. 5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов),методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				

ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
ОДТ. 5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+

ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ. 8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и				

	иных внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС. 5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС. 7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				

ЗИС. 8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				

ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ. 5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+

УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

3.11.3 Результаты и выводы:

Студенты изучили требования к защите персональных данных при их обработке в информационных системах персональных данных

3.12 Практическое занятие № 13 (2 часа).

Тема: «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"»

3.12.1 Задание для работы:

1. Общие положения.
2. Состав и содержание мер по обеспечению безопасности персональных данных.

…….

3.12.2 Краткое описание проводимого занятия:

1. Общие положения.

1. Настоящий документ разработан в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; 2011, N 23, ст. 3263; N 31, ст. 4701) и устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - меры по обеспечению безопасности персональных данных) для каждого из уровней защищенности персональных данных, установленных в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В настоящем документе не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

2. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система) обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

3. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда, применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

6. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

7. Меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328).

2. Состав и содержание мер по обеспечению безопасности персональных данных.

8. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к настоящему документу.

8.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

8.2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

8.3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

8.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

8.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

8.6. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

8.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

8.8. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

8.9. Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

8.10. Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

8.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

8.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

8.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

8.14. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

8.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

9. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;

адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

10. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

11. В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, указанным в пункте 8 настоящего документа, могут применяться следующие меры:

проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

тестирование информационной системы на проникновения;

использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

12. При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

а) для обеспечения 1 и 2 уровней защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия информационной системы с информационнотелекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

б) для обеспечения 3 уровня защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

в) для обеспечения 4 уровня защищенности персональных данных применяются: .

средства вычислительной техники не ниже 6 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;

межсетевые экраны 5 класса.

Для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

13. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 настоящего документа.

3.12.3 Результаты и выводы:

Студенты изучили состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

3.13 Практическое занятие № 14 (2 часа).

Тема: «Нормативно-правовые, морально-этические, административные, физические и технические (программно-аппаратные) меры»

3.13.1 Задание для работы:

1. Нормативно-правовые меры.
2. Морально-этические меры.
3. Административные меры.

…….

3.13.2 Краткое описание проводимого занятия:

1. Нормативно-правовые меры.

Для обеспечения социальной безопасности в масштабах страны, региона, отрасли, организации, семьи или отдельной личности практикой выработаны самые разнообразные способы и средства:

- разведка (мониторинг) ситуации;
- уход от опасности, эвакуация;
- блокирование опасных факторов;
- ликвидация опасных факторов;
- силовое противодействие опасности;
- переговоры;
- совместное устранение причин опасности и иные меры.

Известен и общий алгоритм их применения – вначале необходимо выявить признаки социальных опасностей, затем спрогнозировать и оценить их развитие и последствия, выбрать стратегию поведения, затем на ее основе принять необходимые действия или управленческие решения и организовать их исполнение.

На уровне общества и государства, отдельной организации и даже отдельной семьи такое системное управление должно иметь свою методическую, нормативно-правовую, организационную и структурную основу, руководящие и контролирующие элементы, необходимые материальные ресурсы.

В данном разделе мы рассмотрим нормативно-правовое обеспечение вышеназванных мер защиты от социальных опасностей.

<u>Законодательная основа обеспечения социальной безопасности</u>

По каждому виду социальных угроз разрабатываются законы, которые принимаются Государственной Думой Федерального Собрания РФ, и региональные акты, принимаемые представительными органами субъектов Федерации. Для реализации требований законов принимаются подзаконные акты – Указы Президента РФ, Постановления Правительства, федеральные и местные целевые программы, определяющие порядок их исполнения.

Правовой основой обеспечениясоциальной безопасности в стране является *Конституция РФ* – основной закон государства. Законы и иные правовые акты, принимаемые в РФ, не должны противоречить Конституции РФ. Гарантом Конституции является Президент. Президент издает указы и распоряжения, обязательные для исполнения на всей территории Российской Федерации. Федеральные законы принимаются Государственной думой, рассматриваются Советом Федерации, подписываются и обнародуются Президентом.

Каждая статья Конституции, определяющая цели и принципы обеспечения безопасности личности, общества и государства подкрепляется соответствующим Федеральным законом или кодифицированным сборником законодательных норм – Кодексом РФ.

Во всех кодексах РФ: административном, гражданском, земельном, семейном, трудовом, уголовном и во всех иных обязательно присутствуют главы, регламентирующие соответствующие меры защиты от социальных опасностей.

По всем направлениям обеспечения защиты от опасностей социального характера ежегодно принимаются законы, постановления, о которых будет сказано в последующих разделах.

В качестве примера приведем некоторые законодательные акты и нормативно-правовые документы:

- Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 27.07.2006);

- ФЗ от 12 февраля 1998 г. № 28-ФЗ «О гражданской обороне» (в ред. от 22.08.2004);

- ФЗ от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» (в ред. от 27.07.2006);

- ФЗ от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (в ред. от 27.07.2006);

- ФЗ от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях» (в ред. от 6.07.2006);

- ФЗ от 5 марта 1992 г. № 2446-1 «О безопасности» (в ред. от 02.03.2007);

- ФЗ от 31 мая 1996 г. № 61-ФЗ «Об обороне» (в ред. от 26.06.2007);

- ФЗ от 8 января 1998 г. № 3-ФЗ «О санитарно – эпидемиологическом благополучии населения» (в ред. от 01.12.2007);

- ФЗ от 7 февраля 1992 г. № 2300-1 «О защите прав потребителей» (в ред. от 25.10.2007);

- ФЗ от 2 января 2000 г. № 29-ФЗ «О качестве и безопасности пищевых продуктов» (в ред. от 30.12.2006);

- ФЗ от 30 марта 1999 г. № 52-ФЗ «О наркотических средствах и психотропных веществах» (в ред. от 24.07.2007);

- ФЗ от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

- ФЗ от 24 июля 1999 г. № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних»;

- Положение о координации деятельности правоохранительных органов по борьбе с преступностью. Утверждено Указом Президента РФ от 18 апреля 1996 г. № 567;

- Примерные положения «О социально-реабилитационном центре для несовершеннолетних», «О социальном приюте для детей», «О центре помощи детям, оставшимся без попечения родителей», Утверждены постановлением Правительства РФ от 27 ноября 2000 г. № 896;

- Типовое положение о специальном учебно-воспитательном учреждении для детей и подростков с девиантным поведением. Утверждено постановлением Правительства РФ от 25 апреля 1995 г. № 420.

Далее рассмотрим региональные, федеральные и международные программы по обеспечению

2. Морально-этические меры.

Морально-этические меры защиты информации - традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний;

Нарушитель - это лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства;

Несанкционированное действие - действие субъекта в нарушение установленных в системе правил обработки информации;

Несанкционированный доступ - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;

Объект - пассивный компонент системы, единица ресурса информационной системы, доступ к которому регламентируется правилами разграничения доступа;

Объект защиты - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Организационно-правовые способы нарушения безопасности информации включают:

закупку несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;

невыполнение требований законодательства или нормативных актов и задержки в разработке и принятии необходимых нормативных правовых и технических документов в области безопасности информации.

Организационные меры защиты - это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации;

Организационный контроль эффективности защиты информации - проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Пароль - служебное слово, которое считается известным узкому кругу лиц (одному лицу) и используется для ограничения доступа к информации, в помещение, на территорию;

Пользователь - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе;

Правовые меры защиты информации - действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей;

Программно-математические способы нарушения безопасности информации включают:

внедрение программ-вирусов;

внедрение программных закладок как на стадии проектирования системы (в том числе путем заимствования "зараженного" закладками программного продукта), так и на стадии ее эксплуатации, позволяющих осуществить несанкционированный доступ или действия по отношению к информации и системам ее защиты (блокирование, обход и модификация

систем защиты, извлечение, подмена идентификаторов и т.д.) и приводящих к компрометации системы защиты информации.

3. Административные меры.

Заключаются в определении процедур доступа к защищаемой информации и строгом их выполнении. Контроль над соблюдением установленного порядка возлагается на специально обученный персонал. Административные методы применялись многие века и диктовались здравым смыслом. Чтобы случайный человек не прочитал важный документ, такой документ нужно держать в охраняемом помещении. Чтобы передать секретное сообщение, его нужно посылать с курьером, который готов ценой собственной жизни защищать доверенную ему тайну. Чтобы из библиотеки не пропадали в неизвестном направлении книги, необходимо вести учет доступа к библиотечным ресурсам. Современные административные методы защиты информации весьма разнообразны. Например, при работе с документами, содержащими государственную тайну, сначала необходимо оформить допуск к секретным документам. При получении документа и возврате его в хранилище в журнал регистрации заносятся соответствующие записи. Работа с документами разрешается только в специально оборудованном и сертифицированном помещений. На любом этапе известно лицо, несущее ответственность за целостность и секретность охраняемого документа. Схожие процедуры доступа к информации существуют и в различных организациях, где они определяются корпоративной политикой безопасности. Например, элементом политики безопасности может являться контроль вноса и выноса с территории организации носителей информации (бумажных, магнитных, оптических и др.). Административные методы защиты зачастую совмещаются с законодательными и могут устанавливать ответственность за попытки нарушения установленных процедур доступа.

3.13.3 Результаты и выводы:

Студенты изучили нормативно-правовые, морально-этические, административные, физические и технические (программно-аппаратные) меры.

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ СЕМИНАРСКИХ ЗАНЯТИЙ

Не предусмотрено РУП.