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

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ Б1.Б.1.25 Основы информационной безопасности

Направление подготовки (специальность) **10.05.03 Информационная безопасность автоматизированных систем**

Профиль образовательной программы **Безопасность автоматизированных систем критически важных объектов»**

Форма обучения: ***очная***

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция № 1-2 (4 часа).

Тема: «Основные понятия, термины и определения. Основы государственной политики в области информационной безопасности»

1.1.1 Вопросы лекции:

1. Основы государственной политики в области информационной безопасности.

2. Стратегия национальной безопасности Российской Федерации.

1.1.2 Краткое содержание вопросов:

1.

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.

2.

«**Стратегия национальной безопасности Российской Федерации до 2020 года** и Концепция долгосрочного социально-экономического развития РФ на период до 2020 года - два взаимосвязанных и взаимозависимых стратегических документа, которые являются составными частями единой Стратегии развития России до 2020 года.

Именно поэтому ключевыми целями обеспечения национальной безопасности обозначены вхождение России в среднесрочной перспективе в число пяти стран-лидеров по объему ВВП и достижение необходимого уровня национальной безопасности в экономической и технологической сферах.

Подписанной Президентом РФ Стратегией предусмотрено сосредоточение усилий и ресурсов на таких приоритетах устойчивого развития как:

- повышение качества жизни россиян путем гарантирования личной безопасности, а также высоких стандартов жизнеобеспечения;
- экономический рост, который достигается, прежде всего, путем развития национальной инновационной системы и инвестиций в человеческий капитал;
- наука, технологии, образование, которые развиваются путем укрепления роли государства и совершенствования государственно-частного партнерства;
- развитие прогрессивных технологий и целесообразного воспроизводства природно-ресурсного потенциала страны.

Реализация данных ключевых приоритетов позволит перевести национальную экономику на инновационные рельсы, а значит обеспечить национальную безопасность на долгосрочную перспективу.

В Стратегии предусмотрено, что экономический рост будет достигаться путем развития национальной инновационной системы, импортозамещения, поддержки реального сектора экономики, повышения производительности труда, стимулирования и поддержки развития рынка инноваций, наукоемкой продукции и продукции с высокой добавочной стоимостью, освоения новых ресурсных источников, модернизации приоритетных секторов национальной экономики, совершенствования банковской системы, финансового сектора услуг и межбюджетных отношений в РФ.

Кроме того Стратегия выделяет такие направления обеспечения безопасности, как энергетическая и продовольственная безопасность.

Особенно важно, и это отчетливо отражено в подписанном документе, что достижение целей и выполнение задач, поставленных в Стратегии развития России до 2020 года возможно только при активном участии институтов гражданского общества».

1. 2 Лекция № 2 (2 часа).

Тема: «Аттестация объектов информатизации по требованиям безопасности информации»

1.2.1 Вопросы лекции:

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

2. Порядок проведения аттестации и контроля.

1.2.2 Краткое содержание вопросов:

1.Под объектами информатизации, аттестуемыми по требованиям безопасности информации, понимают автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения, предназначенные для обработки и передачи информации, подлежащей защите, вместе с помещениями, в которых они установлены, а также помещения, предназначенные для ведения конфиденциальных переговоров. [1] То есть к объектам информатизации относятся объекты ТСПИ (технических систем передачи информации).Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов иных нормативно — технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации в пределах его компетенции. [1] Организационную структуру системы аттестации объектов информатизации образуют (рис. 1): 1 федеральный орган по сертификации средств и аттестации объектов информатизации по требованиям безопасности информации; 2 органы по аттестации объектов информатизации по требованиям безопасности информации; 3 испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации; 4 заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации). Рис. 1. Организационная структура системы аттестации объектов

информатизации Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам: обеспечения безопасности информации [4] в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере;противодействия иностранным техническим разведкам на территории Российской Федерации; обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации; защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств [5]; осуществления экспортного контроля. [2] Федеральный орган по сертификации и аттестации осуществляет следующие функции [1]: - 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; - организует периодическую публикацию информации по функционированию системы аттестации объектов по требованиям безопасности информации. Органы по аттестации объектов аккредитуются федеральным органом по сертификации и аттестации и получают от него лицензию на проведение аттестации объектов информатизации. Такими органами могут быть отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры ФСТЭК России. Органы по аттестации: - аттестуют объекты информатизации и выдают «Аттестаты соответствия»; - осуществляют контроль над эксплуатацией аттестованных объектов информатизации и безопасностью информации, циркулирующей на них; - 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 органом по сертификации и аттестации и ежеквартально информируют его о своей деятельности в области аттестации. Испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации по заказам заявителей проводят испытания несертифицированной продукции, используемой на объекте информатизации, подлежащем обязательной аттестации, в соответствии с «Положением о сертификации средств защиты информации по требованиям безопасности информации» [1,6]. Заявители:

- проводят подготовку объекта информатизации аттестации путем необходимых организационно-технических мероприятий по защите информации; - привлекают на договорной основе органы по аттестации для организации и проведения аттестации объекта информатизации; - представляют органам по аттестации необходимые документы и условия 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 информатизации, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган аттестации, приводится в «Аттестате соответствия»; - предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию [1]. Порядок проведения аттестации и контроля Порядок проведения аттестации объектов информатизации требованиям безопасности информации представлен на рис. 2. Заявитель для получения «Аттестата соответствия» заблаговременно направляет в орган по аттестации заявку на проведение аттестации с исходными данными по аттестуемому объекту информатизации. Орган по аттестации рассматривает заявку и на основании исходных данных выбирает схему аттестации, согласовывает ее с заявителем и принимает решение о проведении аттестации объекта информатизации.

Пожалуйста, не забудьте правильно оформить цитату: Гавриленко Д. В. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый. — 2013. — №5. — С. 143-148.

2.

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. 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 ФСТЭК России.

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 Федеральной службой по техническому и экспортному контролю (ФСТЭК России).

Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем конфиденциальности и на период времени, установленными в «Аттестате соответствия».
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.
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.
Аттестация проводится органом по аттестации, который аккредитуется ФСТЭК России.
Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, служебной информации ограниченного распространения, персональных данных (государственные информационные систесы), управления экологически опасными объектами, ведения переговоров по вопросам, содержащим сведения, составляющие государственную тайну или служебную информацию ограниченного распространения.
Аттестации также подлежат объекты информатизации, наличие которых у Заказчика обусловлено требованиями Постановлений Правительства Российской Федерации от 15.08.2006 г № 504, от 31.08.2006г. №532, от 29.12.2007 г № 957.

1. 3 Лекция № 3 (2 часа).

Тема: «Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне". Организационно-технические меры защиты сведений, составляющих государственную тайну»

1.3.1 Вопросы лекции:

1. Перечень сведений, составляющих государственную тайну.

2. Защита государственной тайны.

1.3.2 Краткое содержание вопросов:

1.

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

2.

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.

Система защиты охраняемых государством сведений установлена Законом Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне». В соответствии с требованиями Закона ФСБ России и ФСТЭК России в своих нормативных актах определили состав необходимых документов, а также перечень организационных и технических мер, обязательных для исполнения всеми организациями, обрабатывающими гостайну.

Важной составляющей технических мер по защите гостайны является применение сертифицированных технических, криптографических, программных и других средств защиты информации, предназначенных для защиты гостайны.

Компания «Код Безопасности» предлагает комплекс сертифицированных продуктов, разработанных для современных автоматизированных систем и позволяющих обеспечить защиту гостайны с грифом до «Совершенно секретно» включительно.

Применение продуктов компании «Код Безопасности» для защиты гостайны позволит организации:

- обеспечить надежную защиту и полный контроль процесса обработки гостайны в автоматизированной системе;
- эффективно реализовать специальные требования и рекомендации по защите гостайны, необходимые для проведения обязательной аттестации объектов информатизации.

1. 4 Лекция № 4 (2 часа).

Тема: «Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне". Организационно-технические меры защиты коммерческой тайны»

1.4.1 Вопросы лекции:

1. Охрана конфиденциальности информации.

2. Законодательство Российской Федерации о коммерческой тайне.

1.4.2 Краткое содержание вопросов:

1.

МЕРЫ ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Согласно Федеральному закону «О коммерческой тайне» от29.07.2004 № 89-ФЗ, включают в себя: 1) определение перечня информации, составляющей коммерч ескуютайну; 2) ограничение доступа к информации, составляющей коммерческую тайну, путем установленияпорядка обращения с этой информацией и контроля за с

облюдением такого порядка; 3) учет лиц,получивших доступ к информации, составляющей коммерческую тайну, и/или лиц, которым такаяинформация была предоставлена или передана; 4) регулирование отношений по использованиюинформации, составляющей коммерческую тайну, работниками на основании трудовых договоров иконтрагентами на основании гражданско-
правовых договоров; 5) нанесение на материальные носители(документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна»с указанием обладателя этой информации (для юридических лиц –
полное наименование и местонахождения, для индивидуальных предпринимателей –
фамилия, имя, отчество гражданина, являющегосяиндивидуальным предпринимателем, и место жительства).

2.

Федеральным законом о коммерческой тайне регулируются отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестной конкуренции. Действие Закона распространяется на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

Под коммерческой тайной понимается конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Устанавливается законодательное ограничение на отнесение информации к коммерческой тайне в интересах общества, государства и граждан. Так, режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении сведений о численности, составе работников, системе оплаты труда, об условиях труда, показателях производственного травматизма и профессиональной заболеваемости, наличии свободных рабочих мест, а также задолженности работодателей по выплате заработной платы и по иным социальным выплатам.

Также устанавливается обязательность предоставления на безвозмездной основе органам государственной власти и местного самоуправления по их мотивированному требованию информации, составляющей коммерческую тайну.

Законом определяются права обладателя коммерческой тайны, регулируются отношения, связанные с коммерческой тайной, полученной при выполнении государственного контракта для государственных нужд. Также устанавливаются требования к охране конфиденциальности информации, составляющей коммерческую тайну, в том числе при трудовых отношениях и в гражданско-правовых отношениях.

Предусматривается ответственность за нарушение законодательства РФ о коммерческой

тайне.

Грифы, нанесенные до вступления в силу Закона на материальные носители и указывающие на содержание в них информации, составляющей коммерческую тайну, сохраняют свое действие при условии, если меры по охране конфиденциальности указанной информации будут приведены в соответствие с требованиями Закона.

1. 5 Лекция № 5 (2 часа).

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

1.5.1 Вопросы лекции:

1. Требования к организации защиты информации.

2. Разработка системы защиты информации информационной системы.

1.5.2 Краткое содержание вопросов:

1.

1. Настоящие Требования распространяются на федеральные государственные информационные системы, созданные или используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательные для размещения в информационно-телекоммуникационной сети Интернет, определяемые Правительством Российской Федерации[1] (далее - информационные системы общего пользования), и являются обязательными для операторов информационных систем общего пользования при разработке и эксплуатации информационных систем общего пользования.
2. Информационные системы общего пользования должны обеспечивать:

сохранность и неизменность обрабатываемой информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения (далее - целостность информации);

беспрепятственный доступ пользователей к содержащейся в информационной системе общего пользования информации (далее - доступность информации);

защиту от действий пользователей в отношении информации, не предусмотренных правилами пользования информационной системой общего пользования, приводящих, в том числе к уничтожению, модификации и блокированию информации (далее - неправомерные действия).

3. Информационные системы общего пользования включают в себя средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

4. Информация, содержащаяся в информационной системе общего пользования, является общедоступной.

5. Информационные системы общего пользования в зависимости от значимости содержащейся в них информации и требований к ее защите разделяются на два класса.

5.1. К I классу относятся информационные системы общего пользования Правительства Российской Федерации и иные информационные системы общего пользования в случае, если нарушение целостности и доступности информации, содержащейся в них, может привести к возникновению угроз безопасности Российской Федерации. Отнесение информационных систем общего пользования к I классу проводится по решению руководителя соответствующего федерального органа исполнительной власти.

5.2. Ко II классу относятся информационные системы общего пользования, не указанные в подпункте 5.1 настоящего пункта.

6. Защита информации, содержащейся в информационных системах общего пользования, достигается путем исключения неправомерных действий в отношении указанной информации.

7. Методы и способы защиты информации в информационных системах общего пользования определяются оператором информационной системы общего пользования и должны соответствовать настоящим Требованиям.

Достаточность принятых мер по защите информации в информационных системах общего пользования оценивается при проведении мероприятий по созданию данных систем, а также в ходе мероприятий по контролю за их функционированием.

8. Работы по защите информации в информационных системах общего пользования являются неотъемлемой частью работ по созданию данных систем.

9. Размещение информационных систем общего пользования, специальное оборудование и охрана помещений, в которых находятся технические средства, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей информации и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

10. Защиту информации в информационных системах общего пользования обеспечивает оператор информационной системы общего пользования.

11. В информационных системах общего пользования должны быть обеспечены:

поддержание целостности и доступности информации;

предупреждение возможных неблагоприятных последствий нарушения порядка доступа к информации;

проведение мероприятий, направленных на предотвращение неправомерных действий в отношении информации;

своевременное обнаружение фактов неправомерных действий в отношении информации;

недопущение воздействия на технические средства информационной системы общего пользования, в результате которого может быть нарушено их функционирование;

возможность оперативного восстановления информации, модифицированной или уничтоженной вследствие неправомерных действий;

проведение мероприятий по постоянному контролю за обеспечением их защищенности;

возможность записи и хранения сетевого трафика.

12. Мероприятия по обеспечению защиты информации в информационных системах общего пользования включают в себя:

определение угроз безопасности информации, формирование на их основе модели угроз;

разработку на основе модели угроз системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты информации, предусмотренных для соответствующего класса информационных систем общего пользования;

проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

обучение лиц, использующих средства защиты информации, применяемые в информационной системе общего пользования, правилам работы с ними;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

проведение разбирательств и составление заключений по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению безопасности информации или другим нарушениям, снижающим уровень защищенности информационной системы общего пользования, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

описание системы их защиты.

13. Для разработки и осуществления мероприятий по защите информации в информационных системах общего пользования оператором информационной системы общего пользования назначается структурное подразделение или должностное лицо (работник), ответственные за обеспечение защиты информации.

14. Запросы пользователей на получение информации, содержащейся в информационных системах общего пользования, а также факты предоставления информации по этим запросам регистрируются автоматизированными средствами информационных систем общего пользования в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора информационной системы общего пользования.

15. При обнаружении нарушений порядка доступа к информации оператор информационной системы общего пользования организует работы по выявлению причин

нарушений и устранению этих причин в установленном порядке. Подсистема информационной безопасности должна обеспечивать восстановление информации в информационной системе общего пользования, модифицированной или уничтоженной вследствие неправомерных действий в отношении такой информации. Время восстановления процесса предоставления информации пользователям не должно превышать 8 часов.

16. Реализация требований по обеспечению защиты информации в средствах защиты информации возлагается на их разработчиков.

17. При создании и эксплуатации информационных систем общего пользования должны выполняться следующие требования по защите информации:

17.1. В информационных системах общего пользования I класса:

использование средств защиты информации от неправомерных действий, в том числе средств криптографической защиты информации (электронной цифровой подписи, при этом средства электронной цифровой подписи обязательно должны применяться к публикуемому информационному наполнению), сертифицированных ФСБ России;

использование средств обнаружения вредоносного программного обеспечения, в том числе антивирусных средств, сертифицированных ФСБ России;

использование средств контроля доступа к информации, в том числе средств обнаружения компьютерных атак, сертифицированных ФСБ России;

использование средств фильтрации и блокирования сетевого трафика, в том числе средств межсетевого экранирования, сертифицированных ФСБ России;

осуществление локализации и ликвидации неблагоприятных последствий нарушения порядка доступа к информации;

осуществление записи и хранения сетевого трафика при обращении к государственным информационным ресурсам за десять и более последних дней и предоставление доступа к записям по запросам уполномоченных государственных органов, осуществляющих оперативно-разыскную деятельность;

обеспечение защиты от воздействий на технические и программные средства информационных систем общего пользования, в результате которых нарушается их функционирование, и несанкционированного доступа к помещениям, в которых находятся данные средства, с использованием технических средств охраны, в том числе систем видеонаблюдения, предотвращающих проникновение в помещения посторонних лиц;

осуществление регистрации действий обслуживающего персонала и пользователей;

обеспечение резервирования технических и программных средств, дублирования носителей и массивов информации;

использование сертифицированных в установленном порядке систем обеспечения гарантированного электропитания (источников бесперебойного питания);

осуществление мониторинга их защищенности уполномоченным подразделением ФСБ России;

введение в эксплуатацию только после направления оператором информационной системы общего пользования в ФСБ России уведомления о готовности ввода информационной системы общего пользования в эксплуатацию и ее соответствии настоящим Требованиям.

17.2. В информационных системах общего пользования II класса:

использование средств защиты информации от неправомерных действий, сертифицированных ФСБ России и (или) ФСТЭК России с учетом их компетенции, в том числе средств криптографической защиты информации (электронной цифровой подписи, при этом средства электронной цифровой подписи должны применяться к публикуемому информационному наполнению);

использование средств обнаружения вредоносного программного обеспечения, в том числе антивирусных средств, сертифицированных ФСБ России и (или) ФСТЭК России с учетом их компетенции;

использование средств контроля доступа к информации, в том числе средств обнаружения компьютерных атак, сертифицированных ФСБ России и (или) ФСТЭК России с учетом их компетенции;

использование средств фильтрации и блокирования сетевого трафика, в том числе средств межсетевого экранирования, сертифицированных ФСБ России и (или) ФСТЭК России с учетом их компетенции;

осуществление локализации и ликвидации неблагоприятных последствий нарушения порядка доступа к информации;

осуществление записи и хранения сетевого трафика при обращении к государственным информационным ресурсам за последние сутки и более и предоставление доступа к записям по запросам уполномоченных государственных органов, осуществляющих оперативно-разыскную деятельность;

обеспечение защиты от воздействий на технические и программные средства информационных систем общего пользования, в результате которых нарушается их функционирование, и несанкционированного доступа к помещениям, в которых находятся данные средства;

осуществление регистрации действий обслуживающего персонала;

обеспечение частичного резервирования технических средств и дублирования массивов информации;

использование систем обеспечения гарантированного электропитания (источников бесперебойного питания);

осуществление мониторинга их защищенности уполномоченным подразделением ФСБ России;

введение в эксплуатацию только после направления оператором информационной системы общего пользования в ФСТЭК России уведомления о готовности ввода информационной системы общего пользования в эксплуатацию и ее соответствии настоящим Требованиям.

2.

Государственные (муниципальные) информационные системы (ГИС) – информационные системы, созданные на основании федеральных законов, законов субъектов Российской Федерации, правовых актов государственных органов или решений органов местного самоуправления.

Ключевым документом, устанавливающим обязательные требования к обеспечению защиты информации ограниченного доступа при ее обработке в государственных (муниципальных) информационных системах, является Приказ ФСТЭК России от 11.02.2013 № 17.

Требования этого приказа распространяются, в том числе, и на ГИС, обрабатывающие персональные данные (государственные ИСПДн). По решению обладателя информации (заказчика) или оператора информационной системы требования Приказа № 17 могут применяться и для защиты информации, содержащейся в негосударственных информационных системах.

В соответствии с этими требованиями создание системы защиты информации ГИС осуществляется в следующей последовательности:

- 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 и ввод ее в действие.

Кроме того, при обеспечении информационной безопасности ГИС можно дополнительно руководствоваться Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282.

Следует отметить, что, помимо Приказа ФСТЭК № 17, при создании систем защиты информации государственных информационных систем должны быть учтены и другие нормативные документы, в том числе:

- Постановление Правительства от 1 ноября 2012 г. № 1119;
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К);
- ПКЗ-2005, Приказ № 378 и другие документы ФСБ России;
- национальные и отраслевые стандарты по безопасности информации.

Формирование требований к защите информации ГИС

На этапе формирования требований к защите информации ГИС решаются следующие задачи:

- **Проведение обследования и сбор исходных сведений** об информационной системе, ее характеристиках, структуре, составе, организационно-распорядительной и эксплуатационно-технической документации, а также о реализуемых мероприятиях по обеспечению безопасности информации. Собранные сведения служат основой для дальнейших работ.
- **Классификация информационной системы,**. В соответствии с требованиями Приказа ФСТЭК России от 11.02.2013 № 17 оценивается степень возможного ущерба от нарушения безопасности информации (конфиденциальности, целостности, доступности), уровень значимости информации, масштаб системы. По этим характеристикам определяется требуемый класс защищенности государственной информационной системы.

- **Разработка модели нарушителя и угроз** безопасности информации ГИС. 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.
- **Определение перечня мер обеспечения безопасности, которые должны быть реализованы**. На этом шаге, в соответствии с требованиями ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, осуществляется разработка Технического задания на создание системы защиты информации ГИС, в котором осуществляется выбор, адаптация, уточнение и дополнение защитных мер, содержащихся в Приказе ФСТЭК России от 11.02.2013 № 17 и других нормативных документах по обеспечению безопасности информации ФСТЭК России и ФСБ России.

1. 6 Лекция № 6 (2 часа).

Тема: «Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.12.2013) "О персональных данных". Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

1.6.1 Вопросы лекции:

1. Принципы и условия обработки персональных данных.

2. Меры по обеспечению безопасности персональных данных при их обработке.

1.6.2 Краткое содержание вопросов:

1. Принципы и условия обработки персональных данных.

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.

2. Меры по обеспечению безопасности персональных данных при их обработке.

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

7. Проекты нормативных правовых актов, указанных в части 5 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным.

8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права

ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.
Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

1. 7 Лекция № 7 (2 часа).

Тема: «Нормативно-правовые, морально-этические, административные физические меры. Технические (программно-аппаратные) меры обеспечения безопасности информации»

1.7.1 Вопросы лекции:

1. Технические (программно-аппаратные) меры.

2. Нормативно-правовые меры.

1.7.2 Краткое содержание вопросов:

1. Технические (программно-аппаратные) меры.

Аппаратные средства

Их также называют техническими. По типу они бывают механическими, электронными, электромеханическими и др. С помощью аппаратных средств происходит защита от физического проникновения и маскировка данных, если проникновение все-таки произошло. Защита от проникновения реализовывается с помощью решеток на окнах,

всевозможных замков, сигнализации, сторожа и других средств. Вторую часть задачи выполняют генераторы шума, сканирующие радиоприемники, сетевые фильтры и другие устройства, способные «перекрывать» каналы, по которым может произойти утечка важной информации. Преимущество аппаратных средств состоит в том, что их использование надежно, они не зависят от субъективных факторов, обладают устойчивостью к модификации. Однако существуют и слабые стороны. Они недостаточно гибки, их стоимость довольно высока, масса и размеры сравнительно велики.

Программные средства

В таких средствах встроены специальные программы, за счет которых происходит идентификация пользователя, контролируется доступ, происходит шифровка информации, уничтожается остаточная информация (к примеру, временные файлы), происходит тестовый контроль системы защиты и множество других функций. Среди преимуществ можно поставить акцент на универсальности, надежности, простоте установки, гибкости, возможности модифицировать и развивать данное средство. Среди недостатков – ограниченность в функциональности сети, повышенная чувствительность к изменениям (случайным или преднамеренным), частичное использование рабочих станций или файл-сервера, возможность зависимости от компьютерной техники.

2. Нормативно-правовые меры.

К правовым мерам защиты относятся действующие в стране законы, указы и другие нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.МЕТОДИЧЕСКИЕ УКАЗАНИЯ

ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИЙ ЗАДАНИЙ

2.1 Практическое занятие № 1-2 (6 часов).

Тема: Основные понятия, термины и определения. Основы государственной политики в области информационной безопасности.

2.1.1 Задание для работы:

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

2.1.2 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.

Словосочетание "информационная безопасность" в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин *"информационная безопасность"* используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе РФ "Об участии в международном информационном обмене" (закон утратил силу, в настоящее время действует "Об информации, информационных технологиях и о защите информации") *информационная безопасность* определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

В данном курсе наше внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, на каком языке (русском или каком-либо ином) она закодирована, кто или что является ее источником и какое психологическое воздействие она оказывает на людей. Поэтому термин *"информационная безопасность"* будет использоваться в узком смысле, так, как это принято, например, в англоязычной литературе.

Под ***информационной безопасностью*** мы будем понимать защищенность информации и *поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений, в том числе владельцам и пользователям информации и *поддерживающей инфраструктуры*. (Чуть дальше мы поясним, что следует понимать под *поддерживающей инфраструктурой*.)

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам *информационной безопасности* начинается с выявления *субъектов информационных отношений* и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы *информационной безопасности* – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1. Трактовка проблем, связанных с *информационной безопасностью*, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае "пусть лучше все сломается, чем враг узнает хоть один секретный бит", во втором – "да нет у нас никаких секретов, лишь бы все работало".
2. *Информационная безопасность* не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. *Субъект информационных отношений* может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Возвращаясь к вопросам терминологии, отметим, что термин "компьютерная *безопасность*" (как эквивалент или заменитель *ИБ*) представляется нам слишком узким. Компьютеры – только одна из составляющих информационных систем, и хотя наше внимание будет сосредоточено в первую *очередь* на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее *безопасность* определяется всей совокупностью составляющих и, в первую *очередь*, самым *слабым звеном*, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой *пароль* на "горчичнике", прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от *поддерживающей инфраструктуры*, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта *инфраструктура* имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении *ИБ* перед существительным "*ущерб*" стоит прилагательное "неприемлемый". Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда *стоимость* защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное)*выражение*, а целью защиты информации становится уменьшение *размеров ущерба* до допустимых значений.

2.1.3 Результаты и выводы:

Студенты изучили основные понятия, термины и определения, основы государственной политики в области информационной безопасности.

2.2 Практическое занятие № 4-6 (6 часов).

Тема: Аттестация объектов информатизации по требованиям безопасности информации.

2.2.1 Задание для работы:

1. Общие положения.

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

2.2.2 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.

2.2.3 Результаты и выводы:

Студенты изучили аттестацию объектов информатизации по требованиям безопасности информации.

2.3 Практическое занятие № 7-8 (4 часа).

Тема: Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне". Организационно-технические меры защиты сведений, составляющих государственную тайну.

2.3.1 Задание для работы:

1. Общие положения.

2. Перечень сведений, составляющих государственную тайну.

2.3.2 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)

2.3.3 Результаты и выводы:

Студенты изучили закон РФ от 21.07.1993 N 5485-1 "О государственной тайне". Организационно-технические меры защиты сведений, составляющих государственную тайну.

2.4 Практическое занятие № 9-10 (4 часа).

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

2.4.1 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.

2.4.2 Краткое описание проводимого занятия:

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

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.

2.4.3 Результаты и выводы:

Студенты изучили федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации.

2.5 Практическое занятие № 11-12 (4 часа).

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

2.5.1 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.

2.5.2 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.

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.

2.5.3 Результаты и выводы:

Студенты изучили федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне". Организационно-технические меры защиты коммерческой тайны.

2.6 Практическое занятие № 13-14 (4 часа).

Тема: Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по

обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

2.6.1 Задание для работы:

1. Общие положения.

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

2.6.2 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.

2.6.3 Результаты и выводы:

Студенты изучили защиту информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

2.7 Практическое занятие № 15-16 (4 часа).

Тема: Нормативно-правовые, морально-этические, административные, физические и технические меры.

2.7.1 Задание для работы:

1. Нормативно-правовые меры.
2. Морально-этические меры.
3. Технические меры.

2.7.2 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.

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 социальной безопасности

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. Технические меры.

Технические (программно-аппаратные) меры.

5. К техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, применяемым при предоставлении доступа к информации, распространяемой посредством сети "Интернет", относятся следующие.

5.1. Средства ограничения доступа к техническим средствам доступа к сети "Интернет";

5.2. Средства ограничения доступа к сети "Интернет" с технических средств третьих лиц;

5.3. Средства ограничения доступа к запрещенной для распространения среди детей информации, размещенной на сайтах в сети "Интернет".

2.7.3 Результаты и выводы:

Студенты изучили нормативно-правовые, морально-этические, административные, физические и технические меры