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

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

## Б1.В.11 Технические средства безопасности объектов

**Направление подготовки (специальность)** 27.03.04 Управление в технических системах

**Профиль подготовки (специализация)** Интеллектуальные системы обработки информации и управления

**Квалификация выпускника** бакалавр

**Форма обучения** заочная

**СОДЕРЖАНИЕ**

## 1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция № 1 (2 часа).

Тема: «Предмет и задачи программно-аппаратной защиты информации»

1.1.1 Вопросы лекции:

1. Основные понятия.
2. Уязвимость компьютерных систем.

1.1.2 Краткое содержание вопросов:

1. Основные понятия.

В Федеральном законе РФ «Об информации, информатизации и защите информации», принятом 25 января 1995 года Государственной Думой, определено, что «информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления». Информация имеет ряд особенностей:

• она нематериальна;

• информация хранится и передается с помощью материальных носителей;

• любой материальный объект содержит информацию о самом себе или о другом объекте.

Не материальность информации понимается в том смысле, что нельзя измерить ее параметры известными физическими методами и приборами. Информация не имеет массы, энергии и т. п.

Информация хранится и передается на материальных носителях. Такими носителями являются мозг человека, звуковые и электромагнитные волны, бумага, машинные носители (магнитные и оптические диски, магнитные ленты и барабаны) и др.

Информации присущи следующие свойства.

Информация доступна человеку, если она содержится на материальном носителе. Поэтому необходимо защищать материальные носители информации, так как с помощью материальных средств можно защищать только материальные объекты.

Информация имеет ценность. Ценность информации определяется степенью ее полезности для владельца. Обладание истинной (достоверной) информацией дает ее владельцу определенные преимущества. Истинной или достоверной информацией является информация, которая с достаточной для владельца (пользователя) точностью отражает объекты и процессы окружающего мира в определенных временных и пространственных рамках.

Информация, искаженно представляющая действительность (недостоверная информация), может нанести владельцу значительный материальный и моральный ущерб. Если информация искажена умышленно, то ее называютдезинформацией.
Законом «Об информации, информатизации и защите информации» гарантируется право собственника информации на ее использование и защиту от доступа к ней других лиц (организаций). Если доступ к информации ограничивается, то такая информация является конфиденциальной.
Конфиденциальная информация может содержать государственную или коммерческую тайну. Коммерческую тайну могут содержать сведения, принадлежащие частному лицу, фирме, корпорации и т. п. Государственную тайну могут содержать сведения, принадлежащие государству (государственному учреждению). В соответствии с законом «О государственной тайне» сведениям, представляющим ценность для государства, может быть присвоена одна из трех возможных степеней секретности. В порядке возрастания ценности (важности) информации ей может быть присвоена степень (гриф) «секретно», «совершенно секретно» или «особой важности». В государственных учреждениях менее важной информации может присваиваться гриф «для служебного пользования».
Для обозначения ценности конфиденциальной коммерческой информации используются три категории:
• «коммерческая тайна - строго конфиденциально»;
• «коммерческая тайна - конфиденциально»;
• «коммерческая тайна».
Используется и другой подход к градации ценности коммерческой информации:
• «строго конфиденциально - строгий учет»;
• «строго конфиденциально»;
• «конфиденциально».
Ценность информации изменяется во времени.

2. Уязвимость компьютерных систем.
Уязвимость информации — это возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

Атакой на КС называют действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе говоря, атака на КС является реализацией угрозы безопасности информации в ней.

Угрозы информационной безопасности могут быть разделены на угрозы, не зависящие от деятельности человека(естественные угрозы физических воздействий на информацию стихийных природных явлений), и угрозы, вызванные человеческой деятельностью (искусственные угрозы), которые являются гораздо более опасными.
Искусственные угрозы исходя из их мотивов разделяются на непреднамеренные (случайные) и преднамеренные (умышленные).
К непреднамеренным угрозам относятся:
• ошибки в проектировании КС;
• ошибки в разработке программных средств КС;
• случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения;
• ошибки пользователей КС;
• воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их элек-тромагнитной совместимости) и др.
К умышленным угрозам относятся:
• несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);
• несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

1. 2 Лекция № 2 (2 часа).
Тема: «Политика безопасности в компьютерных системах.»
1.2.1 Вопросы лекции:
1. Основные процессы жизненного цикла АС.
2. Оценка защищенности КС.
3. Взаимосвязь между стандартными процессами и стадиями.

1.2.2 Краткое содержание вопросов:

1. Основные процессы жизненного цикла АС.
Жизненный цикл АСУ определен как совокупность взаимосвязанных процессов создания и последовательного изменения её состояния от формирования исходных требований до окончания эксплуатации и утилизации комплекса средств автоматизации.
Рекомендуемые для описания жизненного цикла АСУ процессы делятся на основные, вспомогательные и организационные.

Основные процессы жизненного цикла АСУ состоят из пяти процессов, которые реализуются заказчиком, поставщиком, разработчиком или какой-то другой стороной, вовлеченной в эту деятельность:

процесс заказа: определяет работы заказчика, то есть организации, которая приобретает систему;

процесс поставки: определяет работы поставщика, то есть организации, которая поставляет систему или её часть;

процесс разработки: определяет работы разработчика, то есть организации, которая проектирует и разрабатывает систему или её часть;

процесс эксплуатации: определяет работы организации, которая обеспечивает эксплуатационное обслуживание системы в заданных условиях в интересах пользователей;

процесс сопровождения: определяет работы персонала, то есть организации, которая предоставляет услуги по сопровождению технических и программных средств, состоящих в контролируемом изменении с целью сохранения их исходного состояния и функциональных возможностей.

Вспомогательный процесс является целенаправленной составной частью другого процесса, обеспечивающей его успешную реализацию и качество выполнения. Вспомогательный процесс, при необходимости, инициируется и используется другим процессом. Вспомогательными процессами являются:

процесс документирования: определяет работы по описанию сформированных требований, полученных результатов и т.п.;

процесс управления конфигурацией: определяет работы по управлению конфигурацией технических и программных средств;

процесс обеспечения качества: определяет работы по объективному обеспечению того, чтобы продукты проектирования и процессы соответствовали установленным для них требованиям и реализовывались в рамках утвержденных планов;

процесс верификации: определяет работы (заказчика, поставщика или независимой стороны) по верификации разработанных продуктов и процессов, то есть их соответствие предъявляемым требованиям, по мере реализации этапов проекта;

процесс аттестации: определяет работы (заказчика, поставщика или независимой стороны) по окончательному утверждению соответствия продуктов проектирования, предъявляемым к ним требованиям;

процесс совместного анализа: определяет работы по оценке состояния и результатов какой-либо деятельности. Данный процесс может использоваться двумя любыми сторонами, когда одна из сторон проверяет другую;
процесс аудита: определяет работы по определению соответствия требованиям, планам и договору. Данный процесс может использоваться, когда одна из сторон контролирует продукты и работы другой стороны;
процесс решения проблемы: определяет работы по анализу и устранению проблем (включая несоответствия), которые были обнаружены во время разработки, эксплуатации или других процессов независимо от их характера и источника.

2.Оценка защищенности КС.

Гостехкомиссией при Президенте Российской Федерации были приняты руководящие документы, посвященные вопросам защиты информации в автоматизированных системах. Основой этих документов является концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации и основные принципы защиты КС.

Для определения принципов защиты информации вводится понятие несанкционированного доступа к информации. Это понятие является чрезвычайно важным, так как определяет, от чего сертифицированные по руководящим документам средства вычислительной техники и КС должны защищать информацию. В соответствии с принятой в руководящих документах классификацией, основными способами НСД являются:

1. непосредственное обращение к объектам доступа (получение процессом, управляемым пользователем доступа к файлу);
2. создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
3. модификация средств защиты, позволяющая осуществить НСД (программные и аппаратные закладки);
4. внедрение в технические средства аппаратных или программных механизмов, нарушающих структуру и функции КС и позволяющие осуществить НСД (загрузка нестандартной операционной системы без функций защиты).

Руководящие материалы представляют семь критериев защиты КС:

1. Защита КС основывается на положениях существующих законов, стандартов и нормативно-методических документов по защите информации.

2. Защита средств вычислительной техники обеспечивается комплексом программно-технических средств.
3. Защита КС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.
4. Защита КС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.
5. Программно-технические средства не должны существенно ухудшать основные функциональные характеристики КС (надежность, производительность, возможность изменения конфигурации).
6. Оценка эффективности средств защиты, учитывающей всю совокупность технических характеристик, включая технические решения и практическую реализацию средств защиты.
7. Защита КС должна предусматривать контроль эффективности средств защиты от НСД, который может быть периодическим или включаться по мере необходимости пользователем или контролирующими органами.

3.Взаимосвязь между стандартными процессами и стадиями.
Основной задачей СЗИ является обеспечение безопасности КС. Безопасность КС и обрабатываемой с их помощью информации является производным понятием от понятия информационной безопасности. При выработке подходов к решению проблемы информационной безопасности следует исходить из того, что конечной целью защиты являются не информация и компьютерные системы, а безопасность всех категорий субъектов, участвующих в информационных процессах, от нанесения им материального, морального или иного ущерба в результате нежелательных (случайных или преднамеренных) воздействий на элементы КС (т.е. нарушения состояния защищенности). В качестве возможных нежелательных воздействий на компьютерные системы могут рассматриваться преднамеренные действия злоумышленников, ошибочные действия обслуживающего персонала и пользователей системы, проявления ошибок в ее программном обеспечении, сбои и отказы оборудования, аварии и стихийные бедствия, которые могут привести к разглашению (нарушению конфиденциальности, незаконному тиражированию), искажению (нарушению целостности), утрате, разрушению или снижению степени доступности информации. При этом именно неправомерное искажение, фальсификация, уничтожение или разглашение определенной части информации, а также дезорганизация процессов ее обработки и передачи в

информационно-управляющих системах может нанести наиболее серьезный ущерб государству, юридическим и физическим лицам, участвующим в информационных процессах. Каждый способ НСД характеризуется множеством программно-аппаратных средств и действий субъектов с использованием этих средств. Человек (субъект НСД) способен придумать принципиально новый способ реализации НСД или применить новые варианты известных способов.

В общем случае все способы НСД являются результатом композиций "первичных" действий, таких как:

-запись информации;

-считывание информации;

-физическое воздействие на элементы компьютерных систем, приводящее либо к уничтожению информации, либо к нарушению правил ее обработки и хранения.

К примеру, несанкционированная модификация информации является композицией чтения и записи информации. Несанкционированное уничтожение информации, как и ее блокирование, может произойти в результате или несанкционированной записи, или физического воздействия на элемент компьютерных систем. Несанкционированное копирование информации осуществляется путем последовательного чтения и записи информации. Подбор пароля состоит в последовательности записи и чтения результатов обработки этой записи, при этом обычно пуск несанкционированного процесса является следствием несанкционированной записи или модификации (чтения и записи) информации.

Все каналы проникновения в систему и утечки информации разделяют на прямые и косвенные. Под косвенными понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы. Для использования прямых каналов такое проникновение необходимо. Прямые каналы могут использоваться без внесения изменений в компоненты системы или с изменениями компонентов. По способу получения информации каналы доступа можно разделить на:

-физический;

-электромагнитный (перехват излучений);

-информационный (программно-математический).

При контактном НСД (физическом, программно-математическом) возможные угрозы информации реализуются путем доступа к элементам КС, к носителям информации, к самой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также путем подключения к линиям связи. При бесконтактном доступе (например, по электромагнитному каналу) возможные угрозы

информации реализуются перехватом излучений аппаратуры КС, в том числе наводимых в токопроводящих коммуникациях и цепях питания, перехватом информации в линиях связи, вводом в линии связи ложной информации, визуальным наблюдением (фотографированием) устройств отображения информации, прослушиванием переговоров персонала КС и пользователей.

1. 3 Лекция № 3 (2 часа).

Тема: «Нормативно-методическое обеспечение создания АС.»

1.3.1 Вопросы лекции:

1. Нормативно-методическое обеспечение АС.
2. Международные стандарты.
3. Стандарты Российской Федерации.

1.3.2 Краткое содержание вопросов:

1. Нормативно-методическое обеспечение АС.

азработка больших проектов связанные с работой коллективов в несколько 10-100 человек из нескольких организаций, возможно при наличии нормативно-методических документов, регламентирующих различные аспекты процессов деятельности разработчиков. Комплекс таких документов называется нормативно-методическое обеспечение. Эти документы регламентируют:

- Порядок разработки, внедрения, сопровождения АС (Устав);
- Общие требования к составу АС, связям между ее компонентами, а также к ее качеству (ТЗ);
- Виды, состав и содержание проектной и рабочей документации (Стандарт).

Все документы НМО классифицируются по следующим признакам:

- Виды регламентаций (Стандарт, РД, положение, инструкция и т. д.);
- Статус регламентирующего документа (международный, отраслевой, предприятия);
- Области действия документов (заказчик, подрядчик);
- Объекту регламентации или методического обеспечения (АС, бизнес-процесс).

Нормативной базой НМО являются:

- Международные стандарты ISO/IEC (International organization of standardization/international electrotechnical commision);
- Стандарты РФ (ГОСТ Р)
- Стандарты организаций (СТ/П) – стандарт предприятия

2.Международные стандарты.

ISO/IEC 27001 — международный стандарт по информационной безопасности, разработанный совместно Международной организацией по стандартизации и Международной электротехнической комиссией. Подготовлен к выпуску подкомитетом SC27 Объединенного технического комитета JTC 1. Стандарт содержит требования в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности (СМИБ). В стандарте ISO/IEC 27001 (ISO 27001) собраны описания лучших мировых практик в области управления информационной безопасностью. ISO 27001 устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы. Настоящий стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения Системы Менеджмента Информационной Безопасности (СМИБ).

Информационная безопасность - сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность.

Конфиденциальность - обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи).

Целостность - обеспечение точности и полноты информации, а также методов её обработки.

Доступность - обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию).

Само понятие «защиты информации» трактуется международным стандартом как обеспечение конфиденциальности, целостности и доступности информации. Основа стандарта ИСО 27001 — система управления рисками, связанными с информацией.

Система управления рисками позволяет получать ответы на следующие вопросы:

на каком направлении информационной безопасности требуется сосредоточить внимание;

сколько времени и средств можно потратить на данное техническое решение для защиты информации.

3. Стандарты Российской Федерации.

Для обеспечения сопоставимости и единства интерпретации программной документации в Советском Союзе была разработана Единая Система Программной Документации (ЕСПД). Ниже приводятся выдержки из головного стандарта системы: ГОСТ 19.001-77 «Общие положения», определяющего назначение, состав и область применения ЕСПД. Единая система программной документации - комплекс государственных стандартов, устанавливающих взаимоувязанные правила разработки, оформления и обращения программ и программной документации. В стандартах ЕСПД устанавливают требования, регламентирующие разработку, сопровождение, изготовление и эксплуатацию программ, что обеспечивает возможность: 1. унификации программных изделий для взаимного обмена программами и применения ранее разработанных программ в новых разработках; 2. снижения трудоемкости и повышения эффективности разработки, сопровождения, изготовления и эксплуатации программных изделий; 3. автоматизации изготовления и хранения программной документации.

В понятие «сопровождение программы» включается: 1. анализ функционирования программы, 2. развитие и совершенствование программы, 3.внесение изменений в нее с целью устранения ошибок.

В состав ЕСПД входят:

1. основополагающие и организационно-методические стандарты;
2. стандарты, определяющие формы и содержание программных документов, применяемых при обработке данных;
3. стандарты, обеспечивающие автоматизацию разработки программных документов.

При переходе к рыночным методам управления экономикой страны отпала необходимость жесткой регламентации формы и содержания программной документации для обеспечения ее сопоставимости. В социалистической экономике дублирование разработок (например, разработка одной и той же программы несколькими авторами) жестко пресекалась, так как вело к необоснованному перерасходу государственных средств. В рыночной экономике, такое дублирование даже приветствуется. Фирмы ведут разработки на свои средства, а потом выставляют конкурирующую продукцию на рынок. Покупатель сам определяет, какую продукцию ему купить. Конкуренция заставляет разработчиков выпускать все более совершенную и качественную продукцию.

В этих условиях изменяется роль стандартов ЕСПД. Их требования остаются обязательными только при определенных условиях7 или в случае, если соблюдение

7 Например, при регистрации программы как объекта интеллектуальной собственности оформление программной документации должно соответствовать требованиям стандартов 19.104-78 и 19.106-78. требований стандарта упомянуто в договоре. В остальных случаях требования стандарта носят рекомендательный характер.

1. 4 Лекция № 4 (2 часа).

Тема: «Основные понятия и концепции.».

1.4.1 Вопросы лекции:

1. Идентификация объекта

2. Защита при обмене сообщениями

1.4.2 Краткое содержание вопросов:

1.Идентификация объекта

Идентификация объекта

Определение характеристик объекта и выявление приложенных к нему воздействий с помощью наблюдения за его входами и выходами и статистической обработки полученных данных. Иными словами, И означает отождествление ему как оригиналу некоторой модели. Таково наиболее общее определение, относящееся к системам разного рода (техническим, экономическим и др.).

Проблема идентификации особо исследуется в эконометрике, где произошла, терминологическая инверсия: принято говорить не об И.о., т.е. рассматриваемой экономической системы, а наоборот, об идентификации модели (причем, обычно модели, построенной в виде так

называемой системы одновременных уравнений). Более того, ряд авторов относит этот термин к отдельному элементу модели, понимая под этим установление самого факта, что данный элемент является существенным (см.Существенные переменные). Например, некоторая экзогенная переменная идентифицируется как действительно оказывающая существенное воздействие на ту или иную эндогенную переменную.

2. Защита при обмене сообщениями

Важным аспектом сетевой безопасности является возможность защиты инфраструктуры единой системы обмена сообщениями. В составе среды единой системы обмена сообщениями есть компоненты, которые должны быть правильно настроены, чтобы

защитить данные, пересылаемые по сети с серверов единой системы обмена сообщениями и на них. Сюда входят такие компоненты, как серверы и телефонные группы единой системы обмена сообщениями. В данном разделе рассматривается, как можно повысить защиту данных и серверов в сети единой системы обмена сообщениями в организации. Необходимо выполнить следующие шаги, помогающие защитить среду единой системы обмена сообщениями и включить безопасность VoIP:

установить роль сервера единой системы обмена сообщениями;

Создайте абонентскую группу единой системы обмена сообщениями и настройте ее на использование безопасности VoIP.

связать серверы единой системы обмена сообщениями с телефонной группой единой системы обмена сообщениями;

экспортировать и импортировать сертификаты, необходимые, чтобы серверами единой системы обмена сообщениями, шлюзами IP и IP-АТС и остальными серверами, на которых запущен Microsoft Exchange Server 2007, мог использоваться протокол MTLS (Mutual Transport Layer Security);

настроить полные доменные имена для используемых шлюзов IP единой системы обмена сообщениями.

Существует несколько методов обеспечения безопасности, с помощью которых можно защитить серверы единой системы обмена сообщениями и сетевой трафик, пересылаемый между шлюзами IP и серверами единой системы обмена сообщениями, а также между серверами единой системы обмена сообщениями и остальными серверами Exchange 2007 в организации. В следующей таблице перечислены некоторые из возможных угроз для инфраструктуры единой системы обмена сообщениями и методы обеспечения безопасности, которые можно реализовать, чтобы защититься от них. Протокол MTLS можно использовать для шифрования трафика VoIP, проходящего в сети между шлюзами IP, IP-АТС и другими серверами Exchange 2007 и серверами единой системы обмена сообщениями. Лучший способ защиты в данном случае — это шифрование данных VoIP с помощью протокола MTLS.

Однако в зависимости от конкретной угрозы безопасности можно также настроить политики IPsec таким образом, чтобы включить шифрование данных между шлюзами IP или IP-АТС и сервером единой системы обмена сообщениями и остальными серверами Exchange 2007 в сети. В некоторых средах использование протокола IPsec может оказаться невозможным, потому что протокол IPsec недоступен или не поддерживается шлюзами IP и IP-АТС. Кроме того, использование протокола IPsec вызывает дополнительную нагрузку на системные ресурсы серверов единой системы обмена

сообщениями. С учетом этих факторов протокол MTLS – лучший выбор для защиты сетевого трафика VoIP в среде единой системы обмена сообщениями.

1. 5 Лекция № 5 (2 часа).

Тема: «Взаимная проверка подлинности пользователей».

1.5.1 Вопросы лекции:

1. механизм запроса-ответа

2. механизм отметки времени

1.5.2 Краткое содержание вопросов:

1. механизм запроса-ответа

Процедура состоит в следующем. Если пользователь А хочет быть уверенным, что сообщения, получае¬мые им от пользователя В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент - за¬прос X (например, некоторое случайное число). При ответе пользователь В должен выполнить над этим элементом некоторую операцию (например, вычислить некоторую функцию ). Это невозможно осуществить заранее, так как пользователю В неиз¬вестно, какое случайное число X придет в запросе. Получив ответ с результатом действий В, пользователь А может быть уверен, что В - подлинный. Недостаток этого метода - возможность уста-новления закономерности между запросом и ответом.

Механизм запрос-ответ используется в более сложной процедуре аутентификации - "рукопожатии".

Процедура "рукопожатия" базируется на указанном выше механизме и заключается во взаимной проверке ключей, используемых сторонами. Иначе говоря, сторо¬ны признают друг друга законными партнерами, если докажут друг другу, что обладают правильными ключами. Процедуру рукопожа¬тия обычно применяют в компьютерных сетях при организации сеанса связи между пользователями, пользователем и хост-компьютером, между хост-компьютерами и т.д.

Рассмотрим в качестве примера процедуру рукопожатия для двух пользователей А и В. (Это допущение не влияет на общность рассмотрения. Такая же процедура используется, когда вступающие в связь стороны не являются пользователями). Пусть применяется симметричная криптосистема. Пользователи А и В разделяют один и тот же секретный ключ . Вся процедура по¬казана на рис. 8.2.

Пусть пользователь А инициирует процедуру рукопожатия, от¬правляя пользователю В свой идентификатор  в открытой форме. Пользователь В, получив идентификатор , находит в базе данных секретный ключ  и вводит его в свою криптосистему.

2. механизм отметки времени

Механизм отметки времени подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети может определить, насколько «устарело» пришедшее сообщение, и решить не принимать его, поскольку оно может быть ложным. В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

Для взаимной проверки подлинности обычно используют процедуру «рукопожатия», в которой стороны признают подлинность друг друга, если докажут, что обладают правильными ключами.

Рассмотрим в качестве примера процедуру рукопожатия для пользователей А и В (в качестве которых могут выступать рабочие станции, сервер и т.п.).

1. 6 Лекция № 6 (2 часа).

Тема: «Схема идентификации Гиллоу-Куискуотера».

1.6.1 Вопросы лекции:

1. Алгоритм идентификации с нулевой передачей знания

1.6.2 Краткое содержание вопросов:

1. Алгоритм идентификации с нулевой передачей знания

Широкое распространение интеллектуальных карт (смарт-карт) для разнообразных коммерческих, гражданских и военных применений (кредитные карты, карты социального страхования, карты доступа в охраняемое помещение, компьютерные пароли и ключи, и т.п.) потребовало обеспечения безопасной идентификации таких карт и их владельцев. Во многих приложениях главная проблема заключается в том, чтобы при предъявлении интеллектуальной карты оперативно обнаружить обман и отказать обманщику в допуске, ответе или обслуживании.

Для безопасного использования интеллектуальных карт разработаны протоколы идентификации с нулевой передачей знаний [121]. Секретный ключ владельца карты становится неотъемлемым признаком его личности. Доказательство знания этого

секретного ключа с нулевой передачей этого знания служит доказательством подлинности личности владельца карты.

5.4.1. Упрощенная схема идентификации с нулевой
передачей знаний

Схему идентификации с нулевой передачей знаний предложили в 1986 г. У.Фейге, А.Фиат и А.Шамир. Она является наиболее известным доказательством идентичности с нулевой передачей конфиденциальной информации.

Рассмотрим сначала упрощенный вариант схемы идентификации с нулевой передачей знаний для более четкого выявления ее основной концепции. Прежде всего выбирают случайное значение модуля n, который является произведением двух больших простых чисел. Модуль n должен иметь длину 512…1024 бит. Это значение n может быть представлено группе пользователей, которым придется доказывать свою подлинность. В процессе идентификации участвуют две стороны:

• сторона А, доказывающая свою подлинность,

• сторона В, проверяющая представляемое стороной А доказательство.

Для того чтобы сгенерировать открытый и секретный ключи для стороны А, доверенный арбитр (Центр) выбирает некоторое число V, которое является квадратичным вычетом по модулю n. Иначе говоря, выбирается такое число V, что сравнение

x2 º V (mod n)

имеет решение и существует целое число

V –1 mod n.

Выбранное значение V является открытым ключом для А. Затем вычисляют наименьшее значение S, для которого

S º sqrt (V –1) (mod n).

Это значение S является секретным ключом для А.

## 3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1 Практическое занятие № 1 (2 часа).
Тема: «Основные понятия»

3.1.1 Задание для работы:

1. Информационные процессы
2. Несанкционированное воздействие

3.1.2 Краткое описание проводимого занятия:

1. В непрозрачной упаковке в случайном порядке хранятся 10 электродов диаметром 3 мм, 20 электродов диаметром 4 мм, 30 электродов диаметром 5 мм и 40 электродов диаметром 6 мм. Какое количество информации будет содержать зрительное сообщение о диаметре вынутого из упаковки электрода?

Решение: Так как количество электродов различных диаметров неодинаково, то зрительные сообщения о диаметре вынутого из упаковки электрода также различаются и равны количеству электродов данного диаметра деленному на общее количество электродов:

10 + 20 + 30 + 40 = 100 - электродов всего,

$P_{3мм} = 10/100$; $P_{4мм} = 20/100$; $P_{5мм} = 30/100$; $P_{6мм} = 40/100$, следовательно:

$P_{3мм} = 0,1$; $P_{4мм} = 0,2$; $P_{5мм} = 0,3$; $P_{6мм} = 0,4$.

События неравновероятны, поэтому для определения количества информации, содержащегося в сообщении о диаметре электрода, воспользуемся формулой Шеннона:

$I = - (0,1 \cdot \log_2 0,1 + 0,2 \cdot \log_2 0,2 + 0,3 \cdot \log_2 0,3 + 0,4 \cdot \log_2 0,4) =$ 1,85 бит.

2. Составьте алгоритмическое и программное обеспечение: 1. Процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста. 15 2. Процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и текстового файла. Учтите регистр вводимого текста. 3. Процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста. 4. Процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и текстового файла. Учтите регистр вводимого текста. 5. Постройте программно таблицу Вижинера и выведите в файл. Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.

3.1.3 Результаты и выводы:
Студент знакомится с основными физическими средствами защиты информации, с их функциями. Решает задачи для закрепления материала.

3.2 Практическое занятие № 2 (2 часа).
Тема: «Уязвимость компьютерных систем»

3.2.1 Задание для работы:

1. ошибки в проектировании КС
2. угроза нарушения конфиденциальности

3.2.2 Краткое описание проводимого занятия:
Понятия : информация, информационная безопасность. Цели и задачи обеспечения информационной безопасности. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.

*Вопросы для обсуждения:*

1. Понятия: информация, информатизация, информационные технологии, информационные ресурсы.
2. Место информационной безопасности в национальной безопасности РФ.
3. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.
4. Виды и источники угроз информационной безопасности РФ.

5. Структура государственной системы обеспечения информационной безопасности РФ.
6. Правовое регулирование информационной сферы в РФ.
7. Основные нормативно-методические материалы.

3.2.3 Результаты и выводы:
В результате практической работы, студент научился решать прикладные задачи, связанные с проектированием КС.

3.3 Практическое занятие № 3 (2 часа).
Тема: «Механизмы защиты»

3.3.1 Задание для работы:

1. Список контроля доступа
2. Идентификация, аутентификация и авторизация субъектов и объектов системы

3.3.2 Краткое описание проводимого занятия:
*Вопросы для обсуждения:*

1. Функциональное построение СЗИ организации и назначение основных подразделений.
2. Элементарные модели СЗИ организации. Семирубежная модель защиты.
3. Последовательность и содержание основных этапов проектирования СЗИ организации.
4. Содержание процесса эксплуатации СЗИ организации.

3.3.3 Результаты и выводы:
В ходе практической работы, студент научился разбираться и оперировать основными понятиями информационной безопасности.

3.4 Практическое занятие № 4 (2 часа).
Тема: «Идентификация и аутентификация пользователя»

3.4.1 Задание для работы:

1. Идентификация
2. Аутентификация

3.4.2 Краткое описание проводимого занятия:

1. Перечислите протоколы строгой аутентификации, основанной на симметричны х алгоритмах.
2. Перечислите протоколы строгой аутентификации, основанной на асимметричны х алгоритмах.
3. Что такое односторонняя аутентификация?
4. Что такое двусторонняя аутентификация?

3.4.3 Результаты и выводы:
В ходе практической работы, студент решал задачи, связанные с аутентификацией и идентификацией. Тем самым, обучающийся более полно понял тему идентификация и аутентификация пользователя.

3.5 Практическое занятие № 5 (2 часа).

Тема: «Протоколы идентификации с нулевой передачей знаний »

3.5.1 Задание для работы:

1. Упрощенная схема идентификации с нулевой передачей знаний
2. Параллельная схема идентификации с нулевой передачей знаний

3.5.2 Краткое описание проводимого занятия:

Рассмотрим работу этого протокола для небольших числовых значений. Если n = 35 (n - произведение двух простых чисел 5 и 7), то возможные квадратичные вычеты будут следующими:

1: $x^2 \equiv 1 \pmod{35}$ имеет решения: x = 1, 6, 29, 34;

4: $x^2 \equiv 4 \pmod{35}$ имеет решения: x = 2, 12, 23, 33;

9: $x^2 \equiv 9 \pmod{35}$ имеет решения: x = 3, 17, 18, 32;

11: $x^2 \equiv 11 \pmod{35}$ имеет решения: x = 9, 16, 19, 26;

14: $x^2 \equiv 14 \pmod{35}$ имеет решения: x = 7, 28;

15: $x^2 \equiv 15 \pmod{35}$ имеет решения: x = 15, 20;

16: $x^2 \equiv 16 \pmod{35}$ имеет решения: x = 4, 11, 24, 31;

21: $x^2 \equiv 21 \pmod{35}$ имеет решения: x = 14, 21;

25: $x^2 \equiv 25 \pmod{35}$ имеет решения: x = 5, 30;

29: $x^2 \equiv 29 \pmod{35}$ имеет решения: x = 8, 13, 22, 27;

30: $x^2 \equiv 30 \pmod{35}$ имеет решения: x = 10, 25.

Заметим, что 14, 15, 21, 25 и 30 не имеют обратных значений по модулю 35, потому что они не являются взаимно простыми с 35.

Составим таблицу квадратичных вычетов по модулю 35, обратных к ним значений по модулю 35 и их квадратных корней.

| V | $V^{-1}$ | $S = \text{sqrt}(V^{-1})$ |
|---|---|---|
| 1 | 1 | 1 |
| 4 | 9 * | 3 |
| 9 | 4 | 2 |
| 11 | 16 | 4 |
| 16 | 11 | 9 ** |
| 29 | 29 | 8 |

Пояснения:

* (4 * 9) mod 35 = 1; ** (9 * 9) mod 35 = 11

Итак, сторона А получает открытый ключ, состоящий из К = 4 значений V:

[4, 11, 16, 29] .

Соответствующий секретный ключ, состоящий из K = 4 значений S:

$$[3, 4, 9, 8] .$$

Рассмотрим один цикл протокола.

1. Сторона A выбирает некоторое случайное число r = 16, вычисляет

$$x = 16^2 \bmod 35 = 11$$

и посылает это значение x стороне B.

2. Сторона B отправляет стороне A некоторую случайную двоичную строку

$$[1, 1, 0, 1] .$$

3. Сторона A вычисляет значение

$$y = r * (S_1^{b_1} * S_2^{b_2} * ...* S_K^{b_K}) \bmod n = 16 * (3^1 * 4^1 * 9^0 * 8^1) \bmod 35 = 31$$

и отправляет это значение y стороне B.

4. Сторона B проверяет, что

$$x = y^2 * (V_1^{b_1} * V_2^{b_2} * ... * V_K^{b_K}) \bmod n = 31^2 * (4^1 * 11^1 * 16^0 * 29^1) \bmod 35 = 11 .$$

Стороны A и B повторяют этот протокол t раз, каждый раз с разным случайным числом r, пока сторона B не будет удовлетворена.

При малых значениях величин, как в данном примере, не достигается настоящей безопасности. Но если n представляет собой число длиной 512 бит и более, сторона B не сможет узнать ничего о секретном ключе стороны A, кроме того факта, что сторона A знает этот ключ.

В этот протокол можно включить идентификационную информацию.

Пусть I - некоторая двоичная строка, представляющая идентификационную информацию о владельце карты (имя, адрес, персональный идентификационный номер, физическое описание) и о карте (дата окончания действия и т.п.). Эту информацию I формируют в Центре выдачи интеллектуальных карт по заявке пользователя A.

Далее используют одностороннюю функцию $f(\cdot)$ для вычисления f(I, j), где j - некоторое двоичное число, сцепляемое со строкой I. Вычисляют значения

$$V_j = f(I, j)$$

для небольших значений j, отбирают K разных значений j, для которых $V_j$ являются квадратичными вычетами по модулю n. Затем для отобранных квадратичных вычетов $V_j$ вычисляют наименьшие квадратные корни из $V_j^{-1} \pmod n$. Совокупность из K значений $V_j$ образует открытый ключ, а совокупность из K значений $S_j$ - секретный ключ пользователя A.

3.5.3 Результаты и выводы:

В ходе практической работы, студент знакомится с задачами на протоколы идентификации с нулевой передачей знаний, а также прикладное применение этих задач. Данная работа позволит более глубже понять и закрепить материал.

3.6 Практическое занятие № 6 (2 часа).

Тема: «Биометрическая идентификация и аутентификация пользователя»

3.6.1 Задание для работы:

1. Системы идентификации по узору радужной оболочки и сетчатки глаз
2. Системы идентификации по отпечаткам пальцев

3.6.2 Краткое описание проводимого занятия:

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **прогнозирования продолжительности жизни пациентов, перенесших сердечный приступ, по данным эхокардиограммы** на основе базы данных репозитория UCI и провести СК-анализ семантической информационной модели.

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **принятие решения о выборе очередного хода в игре "крестики-нолики" в зависимости от расположения крестиков и ноликов** и провести СК-анализ семантической информационной модели.

3.6.3 Результаты и выводы:

В ходе практической работы, студент знакомится с принципами биометрической идентификации и аутентификации пользователя. Также решаются некоторые прикладные задачи.

3.7 Практическое занятие № 7 (2 часа).

Тема: «Парольная аутентификация»

3.7.1 Задание для работы:

1. Одноразовые пароли
2. Генератор паролей

3.7.2 Краткое описание проводимого занятия:

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **классификацию животных по внешним признакам** на основе базы данных репозитория UCI и провести СК-анализ семантической информационной модели

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **диагностику фитопатологии по симптоматике и выработку рекомендаций по плану лечения** на основе информации, содержащейся в учебнике, и провести СК-анализ семантической информационной модели

3.7.3 Результаты и выводы:

В ходе блока практических работ, студент изучает парольную аутентификацию. Благодаря этому, обучающийся узнает более подробно систему аутентификаии.

3.8 Практическое занятие № 8 (2 часа).

Тема: «Система разграничения доступа к информации в кс»

3.8.1 Задание для работы:

1. Матричный подход
2. Полномочный подход

3.8.2 Краткое описание проводимого занятия:

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **прогнозирование успеваемости по ИИС на основе данных по социальному статусу их родителей** и провести СК-анализ семантической информационной модели

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **прогнозирование направления деятельности фирмы на основе данных о расположении и внешнем виде ее офиса** и провести СК-анализ семантической информационной модели

3.7.3 Результаты и выводы:
В ходе блока практических работ, студент изучает систему разграничения доступа к информации в кс. Благодаря этому, обучающийся узнает структуру разграничения доступа к информации в кс.

3.9 Практическое занятие № 9 (2 часа).
Тема: «Методы разграничения доступа »

3.9.1 Задание для работы:
1. Идентификация и аутентификация субъекта доступа
2. Проверка прав доступа субъекта к объекту

3.9.2 Краткое описание проводимого занятия:

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **выбор автомобиля для приобретения по его признакам** (обучающую выборку взять на автомобильном рынке) и провести СК-анализ семантической информационной модели

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **выбор вариантов приобретения жилья по его признакам** и провести СК-анализ семантической информационной модели

3.9.3 Результаты и выводы:
В ходе блока практических работ, студент изучает методы разграничения доступа.
Благодаря этому, обучающийся лучше узнает методы разграничения доступа.

3.10 Практическое занятие № 10 (2 часа).
Тема: «Организация доступа к ресурсам кс»

3.10.1 Задание для работы:
1. Процесс эксплуатации КСЗИ
2. Эксплуатация системы разграничения доступа

3.10.2 Краткое описание проводимого занятия:

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **идентификацию трехмерных тел (шар, куб, тетраэдр, конус, цилиндр, пирамида, призма и других) по их проекциям** и провести СК-анализ семантической информационной модели

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **оценку важности различных видов городского транспорта и**

**различных маршрутов в разрезе по остановкам** и провести СК-анализ семантической информационной модели

3.10.3 Результаты и выводы:
В ходе блока практических работ, студент изучает организацию доступа к ресурсам кс. Благодаря этому, обучающийся лучше узнает организацию ресурсов кс.