Федеральное государственное бюджетное образовательное учреждение
высшего образования «Кемеровский государственный университет»
Новокузнецкий институт (филиал)

Факультет информатики, математики и экономики
Кафедра информатики и вычислительной техники им. В. К. Буторина

О. А. Штейнбрехер

Методы и средства защиты информации

Методические указания по выполнению практических работ по дисциплине «Методы и средства защиты информации» для обучающихся по направлениям подготовки 09.03.03 Прикладная информатика Профиль «Прикладная информатика в экономике» и «Информационная безопасность» и 09.03.01 Информатика и вычислительная техника Профиль «Автоматизированные системы обработки информации и управления»

Новокузнецк
2020

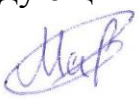
УДК [378.147.88:004.056](072)
ББК 74.484(2Рос-4Кем)я73+32.97я73
Ш88

Ш88 «Методы и средства защиты информации. Методические указания по выполнению практических работ» : метод. указ (текст. электрон. изд.)/ О.А. Штейнбрехер ; Новокузнец. ин-т (фил.) Кемеров. гос. ун-та – Новокузнецк: НФИ КемГУ, 2020. – 67 с.

Приводятся методические указания для выполнения практических работ по дисциплинам «Методы и средства защиты информации» и «Информационная безопасность»: приведены теоретические основы, практические задания, представлены критерии оценки.

Методические указания предназначены для студентов всех форм обучения направлений 09.03.01 «Информатика и вычислительная техника» и 09.03.03 «Прикладная информатика».

Рекомендовано
на заседании кафедры
информатики и вычислительной
техники им. В. К. Буторина
13 марта 2020 года.
Заведующий кафедрой



А. В. Маркидонов

Утверждено
методической комиссией факультета
информатики, математики и экономики
18 мая 2020 года.
Председатель методкомиссии

Г.Н. Бойченко

УДК [378.147.88:004.056](072)
ББК 74.484(2Рос-4Кем)я73+32.97я73

Текст представлен в авторской редакции

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Курсы «Методы и средства защиты информации», «Информационная безопасность» позволяют студентам ознакомиться с методами и средствами защиты информации в персональном компьютере и компьютерных сетях, изучить способы хранения и шифрования данных, проблемы несанкционированного межсетевого доступа к информации, современные средства криптографической защиты информации, вооружиться методами познания и сформировать познавательную самостоятельность. В результате освоения обучающийся должен овладеть следующими результатами обучения по дисциплине.

Знать:

базовые понятия информационной безопасности; классификацию угроз уязвимостей;

нормативно-правовую базу в области защиты информации;

основные понятия и методы организационно-правового, программно-аппаратного, криптографического обеспечения информационной безопасности;

методики построения систем защиты информации.

Уметь:

моделировать угрозы и уязвимости информационной безопасности;

выделять источники информации, объекты защищаемой информации;

формировать требования к построению безопасной системы;

определять функциональные задачи и требования.

Владеть:

методами организационно-правового, программно-аппаратного, криптографического обеспечения информационной безопасности;

методами и методиками построения систем защиты информации;

программными продуктами для оценки риска информационной безопасности;

программными средствами обеспечения информационной безопасности;

протоколами аутентификации, распределения ключей, электронной подписи и финансовой криптографии.

Раздел 1. Введение в предмет. Угрозы информационной безопасности

Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества.

Необходимо иметь в виду, что при рассмотрении проблемы информационной безопасности нарушитель необязательно является злоумышленником. Нарушителем информационной безопасности может быть сотрудник, нарушивший режим информационной безопасности или внешняя среда, например, высокая температура, может привести к сбоям в работе технических средств хранения информации и т. д.

Сформулируем следующее определение "информационной безопасности". Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Рассматривая информацию как товар можно сказать, что нанесение ущерба информации в целом приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и, как следствие, владелец технологии, а может быть и автор, потеряют часть рынка и т. д.

С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т. д.), можно утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления – производстве, транспорте и др.

Именно поэтому при определении понятия "информационная безопасность" на первое место ставится защита информации от различных воздействий.

Поэтому под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.

В ряде случаев понятие "информационная безопасность" подменяется термином "компьютерная безопасность". В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем. Несмотря на это, в рамках изучаемого курса основное внимание будет уделяться изучению вопросов, связанных с обеспечением режима информационной безопасности применительно к вычислительным системам, в которых информация хранится, обрабатывается и передается с помощью компьютеров.

Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

Содержанием информационной безопасности являются целостность, доступность и конфиденциальность информации.

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

1. Обеспечением доступности информации.
2. Обеспечением целостности информации.
3. Обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени. Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно так же получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило.

Целостность информации условно подразделяется на статическую и динамическую. **Статическая** целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. **Динамическая** целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д. Так,

ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности. **Целостность** – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе. **Конфиденциальность** – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

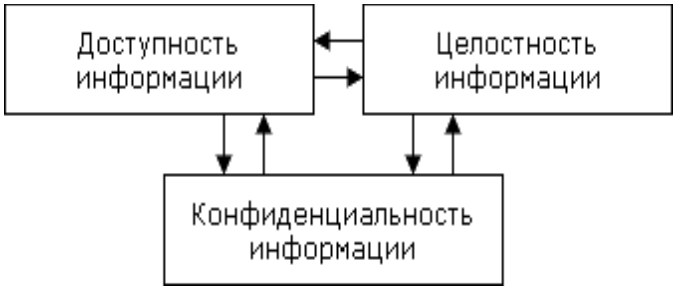


Рисунок 1 – Составляющие информационной безопасности

Система формирования режима информационной безопасности – многоуровневая система, обеспечивающая комплексную защиту информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений.

Анализ основ информационной безопасности показал, что обеспечение безопасности является задачей комплексной. С одной стороны режима информационной, информационная безопасность предполагает, как минимум, обеспечение трех ее составляющих - доступность, целостность и конфиденциальность данных. И уже с учетом этого проблему информационной безопасности следует рассматривать комплексно. С другой стороны, информацией и информационными системами в буквальном смысле "пронизаны" все сферы общественной деятельности и влияние информации на общество все нарастает, поэтому обеспечение информационной безопасности также требует комплексного подхода.

В широком смысле основными задачами информационной безопасности являются:

- защита государственной тайны, т. е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Рассматривая проблему информационной безопасности в узком смысле, отметим, что в этом случае речь идет о совокупности методов и

средств защиты информации и ее материальных носителей, направленных на обеспечение целостности, конфиденциальности и доступности информации.

Исходя из этого, выделим следующие задачи информационной безопасности:

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

С учетом изложенного выделим три уровня формирования режима информационной безопасности:

- законодательно-правовой;
- административный (организационный);
- программно-технический.

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности. Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений. К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированными в законодательном порядке, т. е. в виде свода правил и предписаний. Наиболее характерным примером таких норм является Кодекс

профессионального поведения членов Ассоциации пользователей ЭВМ США. Тем не менее, эти нормы большей частью не являются обязательными, как законодательные меры.

Административный уровень включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации. Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный. Физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам, соответственно к нему относятся технические средства, реализуемые в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решетки и т. д.).

Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу. К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по ключу и т. д. К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например антивирусный пакет и т. д. Программы защиты могут быть как отдельные, так и встроенные. Так, шифрование данных можно выполнить встроенной в операционную систему файловой шифрующей

системой EFS (Windows 2000, XP) или специальной программой шифрования.

Угрозы представляют собой состояния или действия взаимодействующих с носителями информации субъектов и объектов материального мира, которые могут привести к изменению, уничтожению, хищению и блокированию информации. Под блокированием информации понимаются изменения условий хранения информации, которые делают ее недоступной для пользователя. По виду реализации угрозы можно разделить на две группы:

• физическое воздействие внешних сил на источники информации, в результате которого возможны ее изменения, уничтожение, хищение и блокирование;

• несанкционированное распространение носителя с защищаемой информацией от ее источника до злоумышленника, которое приводит к хищению информации.

Угрозы, при реализации которых происходит воздействие различных сил (механических, электрических, магнитных) на источник информации, называются угрозами воздействия на источник информации, а угрозы, приводящие к несанкционированному распространению носителя к злоумышленнику, — угрозами утечки информации. На рисунках 2-3 представлены классификации угроз в зависимости от свойств информации и видов воздействия.

На рисунке 4 представлены источники угроз информационной безопасности.

Рисунок 2 – Виды угроз в зависимости от составляющих информационной безопасности

Рисунок 3 – Классификация угроз информационной безопасности в зависимости от видов воздействий

Уязвимость - это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

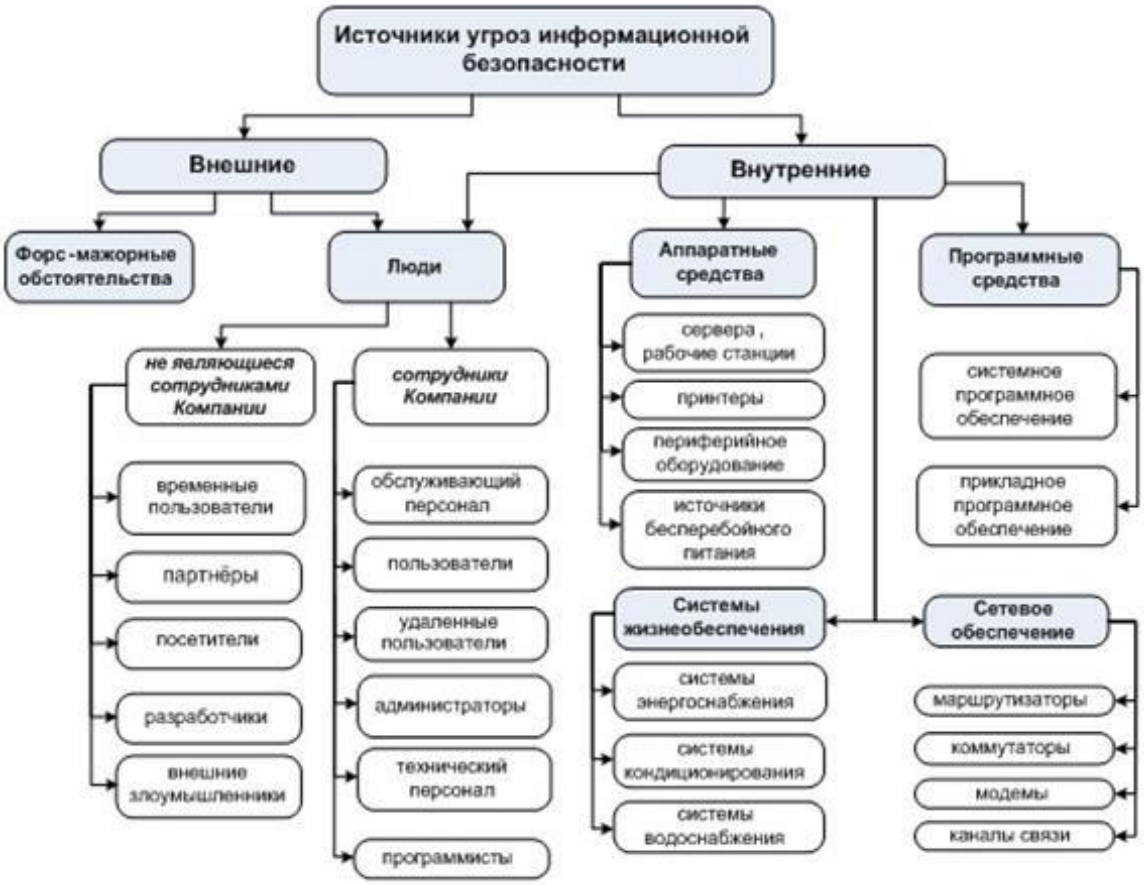


Рисунок 4 – Источники угроз информационной безопасности

Атака - это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.

Практическая работа №1

Построение матрицы рисков для выбранного предприятия.

Цель работы: получение навыков выявления угроз и уязвимостей.

Ход работы:

1. Для предприятия или отдела предприятия выявить носители информации.
2. Для носителя информации выявить угрозы утечки информации и угроз воздействия.
3. Оценить вероятность возникновения угрозы (высокая, средняя, низкая) и уязвимости, которые могут привести к исполнению угрозы.
4. Заполнить таблицу

Информация	Вид	Уязвимое свойство (конфиденциальность, целостность, доступность)	Угроза	Уязвимость

Указания по составлению отчета: отчет должен содержать название работы, цель работы, полученные результаты.

Критерии оценки

Оценка	
Отлично	Задание выполнено без существенных ошибок
Хорошо	Задание выполнено, но допущена одна существенная ошибка, исправленная студентом при указании преподавателя на ошибку
Удовлетворительно	Задание выполнено с наличием одной существенной ошибки, исправленной с помощью преподавателя
Неудовлетворительно	Задание выполнено, но допущено две или более существенные ошибки.

Раздел 2. Основные понятия теории информационной безопасности

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется **атакой** на информационную систему. Лица, преднамеренно реализующие угрозы, являются **злоумышленниками.**

Некоторые угрозы нельзя считать следствием целенаправленных действий вредного характера. Существуют угрозы, вызванные случайными ошибками или техногенными явлениями.

Знание возможных угроз информационной безопасности, а также уязвимых мест системы защиты, необходимо для того, чтобы выбрать наиболее экономичные и эффективные средства обеспечения безопасности.

Угрозы информационной безопасности классифицируются по нескольким признакам:

- **по составляющим информационной безопасности** (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;
- **по компонентам информационных систем**, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- **по характеру воздействия** (случайные или преднамеренные, действия природного или техногенного характера);
- **по расположению источника угроз** (внутри или вне рассматриваемой информационной системы).

Отправной точкой при анализе угроз информационной безопасности является определение составляющей информационной безопасности, которая может быть нарушена той или иной угрозой: конфиденциальность, целостность или доступность.

Все виды угроз, классифицируемые по другим признакам, могут воздействовать на все составляющие информационной безопасности.

Рассмотрим угрозы **по характеру воздействия**.

Опыт проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы.

Причинами *случайных воздействий* при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия злоумышленника. В качестве злоумышленника могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами, например:

- недовольством служащего служебным положением;
- любопытством;
- конкурентной борьбой;
- уязвленным самолюбием и т. д.

Угрозы, классифицируемые **по расположению источника угроз,** бывают внутренние и внешние.

Внешние угрозы обусловлены применением вычислительных сетей и создание на их основе информационных систем.

Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов

обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.

Одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющим нанести ущерб любой из составляющих информационной безопасности является **несанкционированный доступ**. Несанкционированный доступ возможен из-за ошибок в системе защиты, нерационального выбора средств защиты, их некорректной установки и настройки.

Каналы НСД классифицируются по компонентам автоматизированных информационных систем:

Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.

Через программу:

- перехват паролей;
- расшифровка зашифрованной информации;
- копирование информации с носителя.

Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т. д.

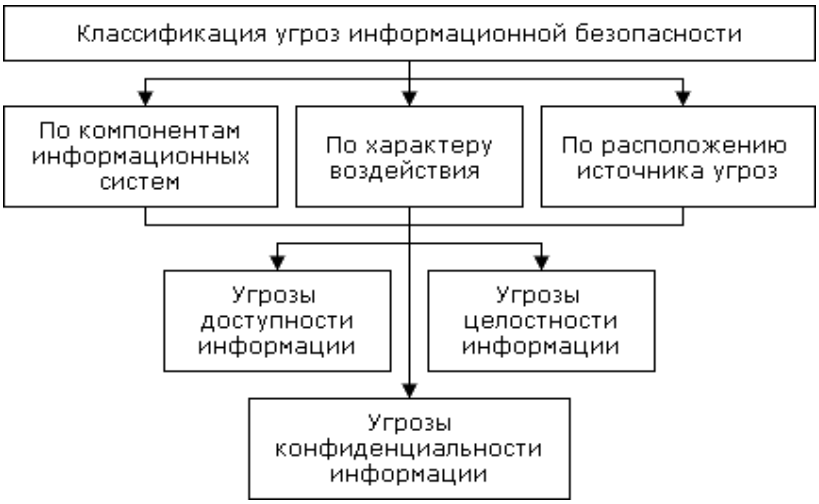


Рисунок 5 – Классификация угроз информационной безопасности

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации.

Административный уровень является промежуточным между законодательно-правовым и программно-техническим уровнями формирования режима информационной безопасности. Законы и стандарты в области информационной безопасности являются лишь отправным нормативным базисом информационной безопасности. Основой практического построения комплексной системы безопасности является административный уровень, определяющий главные направления работ по защите информационных систем.

Задачей административного уровня является разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.

Кроме этого, что немаловажно, именно на административном уровне определяются механизмы защиты, которые составляют третий уровень информационной безопасности – программно-технический.

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения в конкретных условиях функционирования информационной системы.

Содержанием административного уровня являются следующие мероприятия:

1. Разработка политики безопасности.
2. Проведение анализа угроз и расчета рисков.

Разработка политики безопасности ведется для конкретных условий функционирования информационной системы. Как правило, речь идет о политике безопасности организации, предприятия или учебного заведения. С учетом этого рассмотрим следующее определение политики безопасности.

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Основные направления разработки политики безопасности:

- определение объема и требуемого уровня защиты данных;
- определение ролей субъектов информационных отношений.

При описании области применения политики безопасности перечисляются компоненты автоматизированной системы обработки, хранения и передачи информации, подлежащие защите.

В состав автоматизированной информационной системы входят следующие компоненты:

- **аппаратные средства** – компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – дисководы, принтеры, контроллеры), кабели, линии связи и т. д.;
- **программное обеспечение** – приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;
- **данные** – хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;
- **персонал** – обслуживающий персонал и пользователи.

Цели, задачи, критерии оценки информационной безопасности определяются функциональным назначением организации. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т. д.

Политика безопасности затрагивает всех субъектов информационных отношений в организации, поэтому на этапе разработки политики безопасности очень важно разграничить их права и обязанности, связанные с их непосредственной деятельностью.

С точки зрения обеспечения информационной безопасности разграничение прав и обязанностей целесообразно провести по следующим группам (ролям):

- специалист по информационной безопасности;
- владелец информации;
- поставщики аппаратного и программного обеспечения;
- менеджер отдела;
- операторы;

- аудиторы.

В зависимости от размеров организации, степени развитости ее информационной системы, некоторые из перечисленных ролей могут отсутствовать вообще, а некоторые могут совмещаться одним и тем же физическим лицом.

Специалист по информационной безопасности (начальник службы безопасности, администратор по безопасности) играет основную роль в разработке и соблюдении политики безопасности предприятия. Он проводит расчет и перерасчет рисков, выявляет уязвимости системы безопасности по всем направлениям (аппаратные средства, программное обеспечение и т. д.).

Владелец информации – лицо, непосредственно владеющее информацией и работающее с ней. В большинстве случае именно владелец информации может определить ее ценность и конфиденциальность.

Поставщики аппаратного и программного обеспечения обычно являются сторонними лицами, которые несут ответственность за поддержание должного уровня информационной безопасности в поставляемых им продуктах.

Администратор сети – лицо, занимающееся обеспечением функционирования информационной сети организации, поддержанием сетевых сервисов, разграничением прав доступа к ресурсам сети на основании соответствующей политики безопасности.

Менеджер отдела является промежуточным звеном между операторами и специалистами по информационной безопасности. Его задача – своевременно и качественно инструктировать подчиненный ему персонал обо всех требованиях службы безопасности и следить за их выполнением на рабочих местах. Менеджеры должны доводить до подчиненных все аспекты политики безопасности, которые непосредственно их касаются.

Операторы обрабатывают информацию, поэтому должны знать класс конфиденциальности информации и какой ущерб будет нанесен организации при ее раскрытии.

Аудиторы – внешние специалисты по безопасности, нанимаемые организацией для периодической проверки функционирования всей системы безопасности организации.

Практическая работа №2

Нормативные основы информационной безопасности

Цель работы: Знакомство с основными направлениями работ в рамках федеральной программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки ЭЦП.

Ход работы:

1. Подготовить краткое сообщение и тестовые вопросы на темы:

1. Концепции информационного общества
2. Концепция информационного общества в европейской культуре (общество знаний)
3. Государственная программа «Информацио́нное о́бщество» — (государственная программа Российской Федерации, разработанная для создания целостной и эффективной системы использования информационных технологий, при которой граждане получают максимум выгод.) Принята распоряжением Правительства России №1815-р от 20 октября 2010 года.
4. Новые механизмы власти в информационном обществе (концепции М.Фуко, О.Тоффлера, Д.Белла).
5. Электронное правительство: международный опыт и модели реализации в России.
6. Всемирный Саммит по информационному обществу (2003, 2005). Индекс ООН готовности стран к электронному правительству.
7. Концепция правительственной реформы в США.

2. Рассмотреть и проанализировать документы:

1. Постановление Правительства РФ от января 2002 г. N 65 «О федеральной целевой программе «Электронная Россия» (2002-2010 годы)»
2. Постановление Правительства РФ от 10 сентября 2009 г.N 721 «О внесении изменений в федеральную целевую программу «Электронная Россия (2002 - 2010 годы)»

3. Постановление Правительства РФ от 15.08.2006 N 502 «О внесении изменений в ФЦП «Электронная Россия» (2002-2010 годы)”

4. Распоряжение Правительства РФ № 1024-р от 17 июля 2006 года (Концепция региональной автоматизации до 2010 года)

5. Распоряжение Правительства РФ № 1244-р от 27 сентября 2004 года (Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года)

6. Распоряжение Правительства РФ №1555р от 17.10.2009 “План перехода на предоставление государственных услуг и исполнение государственных функций в электронном виде федеральными органами исполнительной власти”

7. Стратегия развития информационного общества в Российской Федерации (Утверждена Президентом Российской Федерации В.Путиным 7 февраля 2008 г., № Пр-212)

Критерии оценки

Оценка	
Отлично	Тема раскрыта полностью, вынесены основные особенности и аспекты нормативных документов
Хорошо	При анализе источников и нормативных документов допущены неточности, не все аспекты раскрыты
Удовлетворительно	Тема раскрыта не в полном объеме, допущены неточности
Неудовлетворительно	Задание выполнено, но допущены существенные ошибки.

Практическая работа №3

Сетевая безопасность

Цель работы: Применение навыков работы с сетевыми протоколами для определения разрешающих правил и администрирования сети.

Ход работы:

1. Опишите настройки межсетевого экрана Windows Server
2. Определите новые разрешающие правила
3. Запретите отправку ICMP-пакетов на один из узлов

Указания по составлению отчета: отчет должен содержать название работы, цель работы, полученные результаты.

Критерии оценки

Оценка	
Отлично	Задание выполнено без существенных ошибок
Хорошо	Задание выполнено, но допущена одна существенная ошибка, исправленная студентом при указании преподавателя на ошибку
Удовлетворительно	Задание выполнено с наличием одной существенной ошибки, исправленной с помощью преподавателя
Неудовлетворительно	Задание выполнено, но допущено две или более существенных ошибок.

Раздел 3. Программно-технические методы защиты

На практике меры защиты информации выделяют относительно способов защиты (рисунок 6). Способы защиты информации — это совокупность приемов и средств, обеспечивающих конфиденциальность, целостность, полноту и доступность информации, и противодействие внутренним и внешним угрозам. Выделяют следующие способы.

- Препятствие - создание на пути угрозы преграды, преодоление которой сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора.
- Управление - оказание управляющих воздействий на элементы защищаемой системы.
- Маскировка - действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника. (Сюда можно, в частности, отнести криптографические методы защиты).
- Регламентация - разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые существенно затрудняют реализацию атак злоумышленника или воздействия других дестабилизирующих факторов.
- Принуждение - метод заключается в создании условий, при которых пользователи и персонал вынуждены соблюдать условия обработки информации под угрозой ответственности (материальной, уголовной, административной)
- Побуждение - метод заключается в создании условий, при которых пользователи и персонал соблюдают условия обработки информации по морально-этическим и психологическим соображениям.

Среди средств защиты выделяют формальные и неформальные средства защиты. К формальным относятся технические и программные средства. Физические средства - механические, электрические,

электромеханические, электронные, электронно-механические и т. п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов. Аппаратные средства - различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации. Программные средства - специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации.

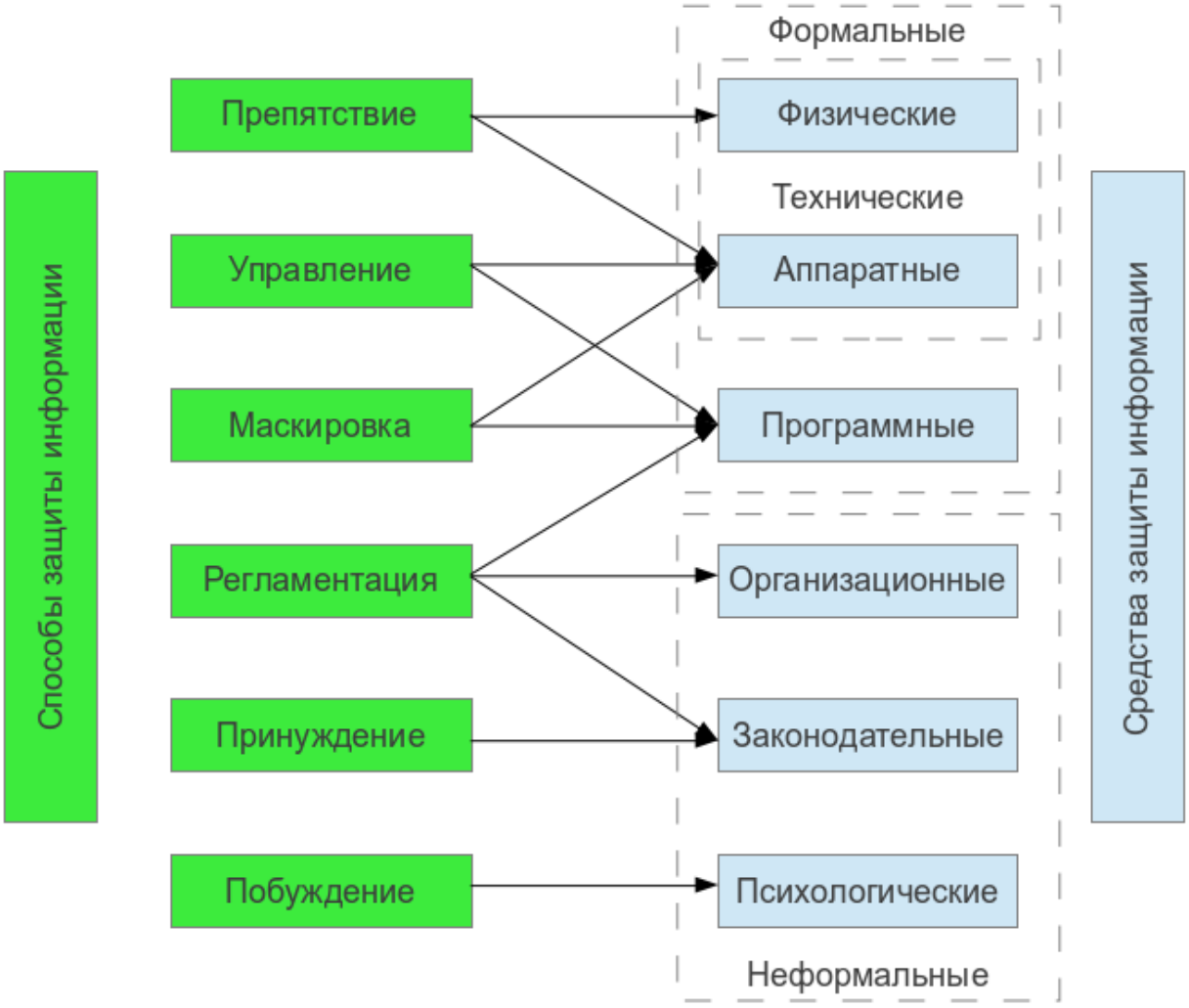


Рисунок 6 – Способы и средства защиты информации

Неформальные средства защиты основаны на регламентации, побуждении и принуждении – организационные, законодательные и психологические средства защиты. Организационные средства -

организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации. Законодательные средства - нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности. Психологические (морально-этические средства) - сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

Рассмотрим формальные средства защиты информации. К физическим средствам защиты относятся экранирование помещений для защиты от излучения, проверка поставляемой аппаратуры на соответствие ее спецификациям и отсутствие аппаратных “жучков”, средства наружного наблюдения, устройства, блокирующие физический доступ к отдельным блокам компьютера, различные замки и другое оборудование, защищающие помещения, где находятся носители информации, от незаконного проникновения и т.д.

Технические средства информационной безопасности реализуются программным и аппаратным обеспечением вычислительных сетей. Такие средства, называемые также службами сетевой безопасности, решают самые разнообразные задачи по защите системы, например контроль доступа, включающий процедуры аутентификации и авторизации, аудит, шифрование информации, антивирусную защиту, контроль сетевого графика и много других задач. Технические средства безопасности могут быть, либо встроены в программное (операционные системы и приложения) и аппаратное (компьютеры и коммуникационное оборудование) обеспечение

сети, либо реализованы в виде отдельных продуктов, созданных специально для решения проблем безопасности. На рисунке 7 приведена классификация инженерно-технических средств защиты информации.

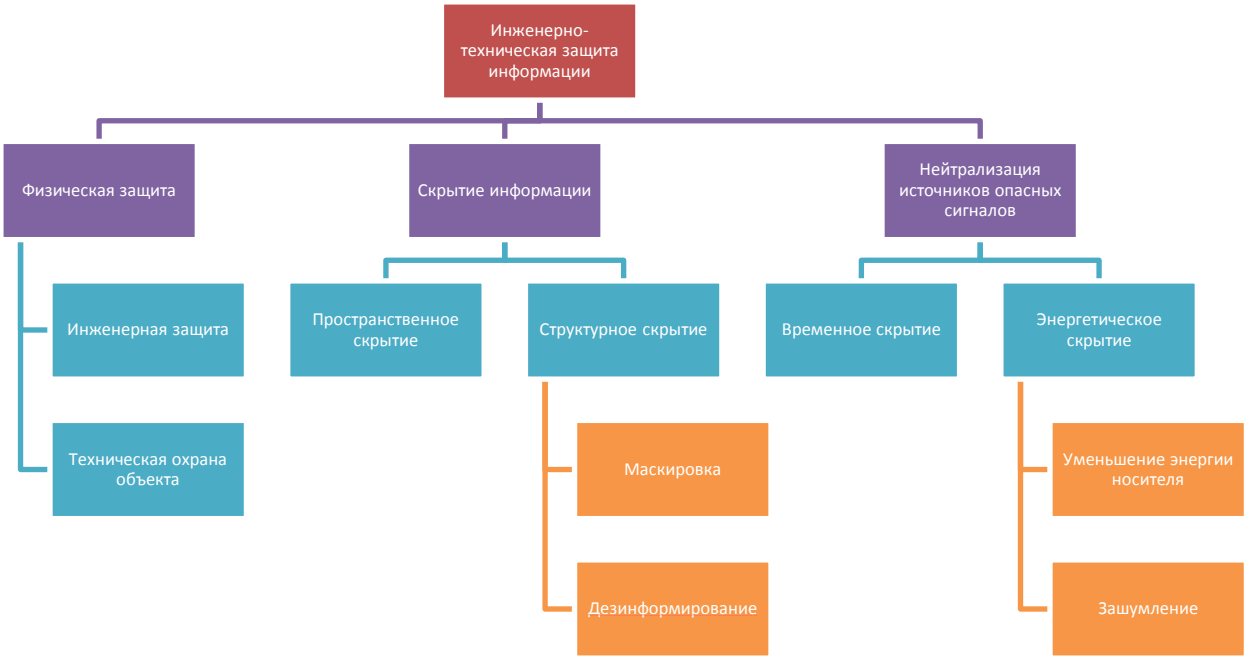


Рисунок 7 – Классификация средств инженерно-технической защиты информации

К группе «скрытие» относятся:

· пассивное скрытие – заключается в исключении или значительном затруднении обнаружения объектов;

· активное скрытие – в создании техническим средствам разведки маскирующих шумовых помех различной физической природы и ложной обстановки по физическим полям;

· специальная защита – заключается в скремблирование телефонных переговоров, кодирование цифровой информации криптографическими методами, программные методы модификации информации.

К группе «дезинформирование» относятся:

· техническая дезинформация;

· имитация;

· легендирование.

При разработке инженерно-технических средств защиты информации требуется выделение зон нахождения носителей информации для учета траектории движения злоумышленника и времени проникновения к источнику информации. Различаются независимые, пересекающиеся и вложенные зоны (рисунок 8).

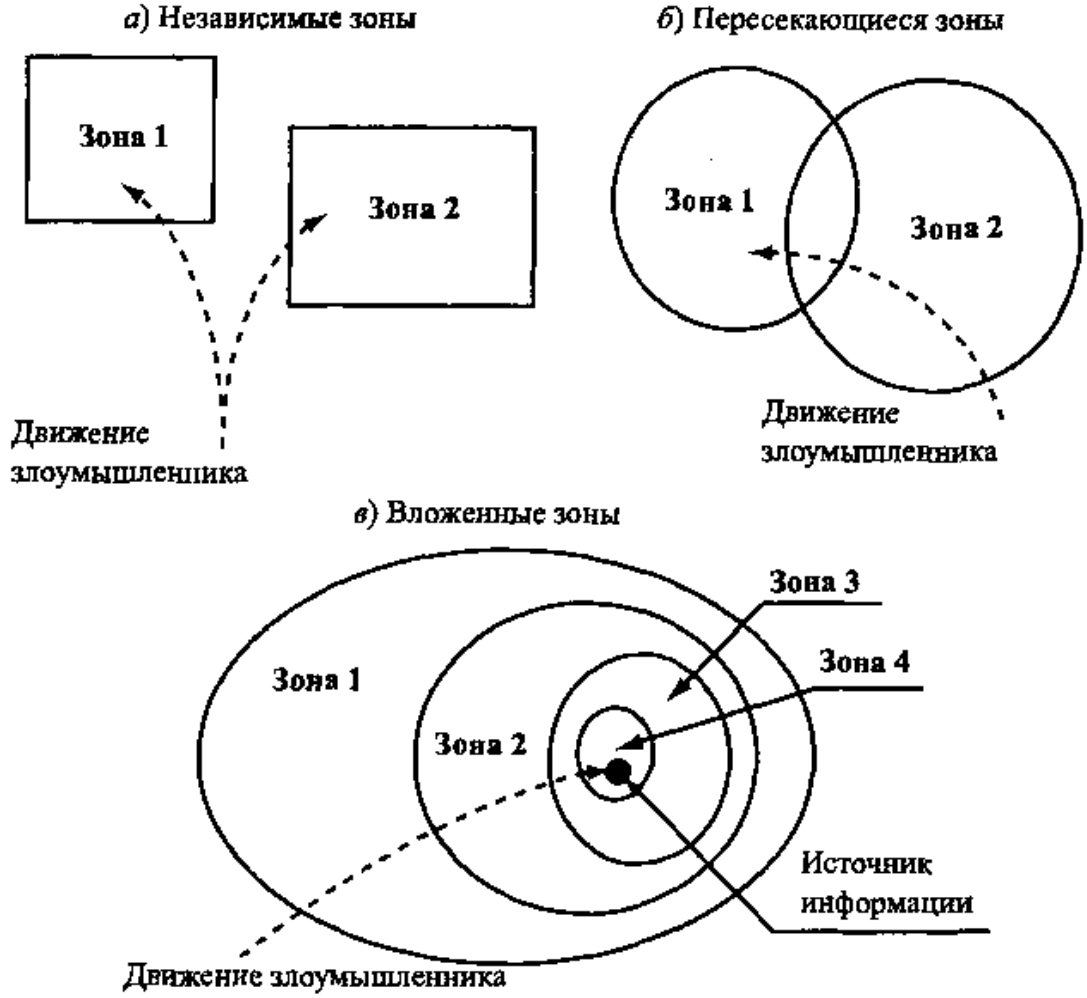


Рисунок 8 – Зонирование территории для организации физической зашиты

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не инженерно-техническим средствам защиты является

именно обязательное включение аппаратных средств в состав технических средств КС. Примеры аппаратных средств защиты информации:

• устройства для хранения информации, идентифицирующей и аутентифицирующей пользователя компьютерной системы (смарт-карты, электронные ШВ-ключи; генераторы одноразовых паролей и т. п.);

• устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.);

• устройства для шифрования информации;

• устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы);

• устройства уничтожения информации на магнитных и иных носителях;

• устройства сигнализации о попытках несанкционированных действий пользователей КС и др.

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций. Примеры программных средств защиты информации:

• программы идентификации и аутентификации пользователей КС;

• программы разграничения доступа пользователей к ресурсам КС;

• программы шифрования информации;

• программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования;

• программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);

• программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановить и доказать факт происшествия этих событий;

• программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);

• программы тестового контроля защищенности КС и др.

К преимуществам программных средств защиты информации относятся:

• простота тиражирования;

• гибкость (возможность настройки на различные условия применения, учитывающие специфику угроз информационной безопасности конкретных КС);

• простота применения — одни программные средства, например, шифрования, работают в «прозрачном» (незаметном для пользователя) режиме, а другие не требуют от пользователя никаких новых (по сравнению с другими программами) навыков;

• практически неограниченные возможности развития путем внесения изменений для учета новых угроз безопасности информации и исправления обнаруженных уязвимостей.

К недостаткам программных средств защиты информации следует отнести:

• снижение эффективности КС за счет потребления ее ресурсов, требуемых для функционирования программ защиты;

• более низкая производительность (по сравнению с выполняющими аналогичные функции аппаратными средствами защиты, например, шифрования);

• возможность злоумышленного изменения программных средств защиты в процессе эксплуатации КС.

Механизмы аутентификации позволяют проверить подлинность личности участника взаимодействия безопасным и надежным способом.

Таблица 1 – Механизмы аутентификации пользователя

Тип	Описание
Пароли или PIN-коды (персональные идентификационные номера)	Что-то, что знает пользователь и что также знает другой участник взаимодействия. Обычно аутентификация производится в 2 этапа. Может организовываться обмен паролями для взаимной аутентификации.
Одноразовый пароль	Пароль, который никогда больше не используется. Часто используется постоянно меняющееся значение, которое базируется на постоянном пароле.
CHAP (протокол аутентификации запрос-ответ)	Одна из сторон инициирует аутентификацию с помощью посылки уникального и непредсказуемого значения "запрос" другой стороне, а другая сторона посылает вычисленный с помощью "запроса" и секрета ответ. Так как обе стороны владеют секретом, то первая сторона может проверить правильность ответа второй стороны.
Встречная проверка (Callback)	Телефонный звонок серверу и указание имени пользователя приводит к тому, что сервер затем сам звонит по номеру, который указан для этого имени пользователя в его конфигурационных данных.

Практическая работа №4

Физическая и инженерно-техническая защита информации

Цель работы: получение навыков планирования и разработки инженерно-технических мер защиты информации

Ход работы:

1. Выделить угрозы и уязвимости, которые можно устранить физическими и инженерно-техническими средствами.

2. Построить схему объекта. Выделить источники защищаемой информации. Определить зоны, классифицировать их (независимые, пересекающиеся, вложенные).

3. Построить движение злоумышленника до источника. Описать возможные меры физической защиты для увеличения времени проникновения.

4. Определить угрозы утечек по техническим, аудио- и видео- каналам. Описать возможные меры инженерно-технической защиты для нейтрализации.

5. Оценить вероятность каждой меры предотвратить уязвимость.

Указания по составлению отчета: отчет должен содержать название работы, цель работы, полученные результаты.

Критерии оценки

Оценка	
Отлично	Задание выполнено без существенных ошибок
Хорошо	Задание выполнено, но допущена одна существенная ошибка, исправленная студентом при указании преподавателя на ошибку
Удовлетворительно	Задание выполнено с наличием одной существенной ошибки, исправленной с помощью преподавателя

Практическая работа №5

Исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль

Цель работы: получение навыков применения и оценки парольной аутентификации пользователей

Ход работы:

1. Составить организационные и управленческие требования для системы аутентификции

2. Описать необходимые алгоритмы хранения и оценки сложности паролей

3. Описать необходимые программные и аппаратные средства

Указания по составлению отчета: отчет должен содержать название работы, цель работы, полученные результаты.

Критерии оценки

Оценка	
Отлично	Задание выполнено без существенных ошибок
Хорошо	Задание выполнено, но допущена одна существенная ошибка, исправленная студентом при указании преподавателя на ошибку
Удовлетворительно	Задание выполнено с наличием одной существенной ошибки, исправленной с помощью преподавателя
Неудовлетворительно	Задание выполнено, но допущено две или более существенных ошибок.

Раздел 4. Криптографические методы защиты

Криптографическими средствами защиты называются специальные средства, методы и алгоритмы преобразования информации, в результате которых маскируется (изменяется по форме представления и скрывается по составу и структуре) ее истинное содержание. Основными видами криптографического преобразования (иначе – закрытия) являются шифрование и кодирование защищаемой информации.

Шифрование - есть такой вид закрытия (преобразования) информации, при котором самостоятельному преобразованию подвергается каждый символ закрываемой информации или передаваемого сообщения;

Кодирование - предназначено для защиты информации, где данные делятся на блоки, имеющие смысловое значение, и каждый такой блок заменяется цифровым, буквенным или комбинированным кодом.

При этом используется несколько различных систем шифрования: заменой, перестановкой, аналитическим преобразованием шифруемой информации. Широкое распространение получили комбинированные шифры, когда исходный текст последовательно преобразуется с использованием двух или даже трех различных шифров. Типичный пример изображения ситуации, в которой возникает задача криптографии (шифрования) изображён на рисунке 9.

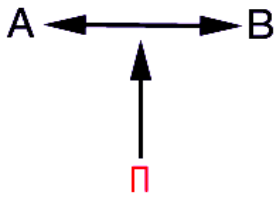


Рисунок 9 – Канал связи с несанкционированным доступом

На рисунке 9 А и В - законные пользователи защищённой информации, они хотят обмениваться информацией по общедоступному каналу связи. П - незаконный пользователь (противник, хакер, конкурент), который хочет

перехватывать передаваемые по каналу связи сообщения и попытаться извлечь из них интересную для него информацию. Эту простую схему можно считать моделью типичной ситуации, в которой применяются криптографические методы защиты информации или просто шифрование.

Исторически в криптографии закрепились некоторые военные слова (противник, атака на шифр, разведданные и так далее). Они наиболее точно отражают смысл соответствующих криптографических понятий. Вместе с тем широко известная военная терминология, основанная на понятии кода (военно-морские коды, коды Генерального штаба, кодовые книги, кодобозначения), уже сравнительно редко применяется в теоретической криптографии. Дело в том, что за последние десятилетия сформировалась теория кодирования - большое научное направление, которое разрабатывает и изучает методы защиты информации от случайных искажений и помех в каналах связи. В таких случаях принято говорить об активных и случайных противниках.

Криптография занимается методами преобразования информации, которые бы не позволили противнику извлечь ее из перехватываемых сообщений. При этом по каналу связи передается уже не сама защищаемая информация, а результат ее преобразования с помощью шифра, и для противника возникает сложная задача вскрытия шифра.

Вскрытие (взлом) шифра - процесс получения защищаемой информации из шифрованного сообщения без предварительного знания примененного шифра.

Под ключом в криптографии понимают сменный элемент шифра, который применяется для шифрования конкретного сообщения.

В последнее время безопасность защищаемой информации стала определяться в первую очередь ключом. Сам шифр, программа шифрования, шифромашина или принцип шифрования стали считать известными противнику и доступными для предварительного изучения, но в них

появился неизвестный для противника ключ, от которого существенно зависят применяемые преобразования информации. Теперь законные пользователи, прежде чем обмениваться шифрованными сообщениями, должны тайно от противника обменяться ключами или установить одинаковый ключ на обоих концах канала связи. А для противника появилась новая задача - определить ключ, после чего можно легко прочитать зашифрованные на этом ключе сообщения. Вернемся к формальному описанию основного объекта криптографии (рисунок 9). Теперь в него необходимо внести существенное изменение - добавить недоступный для противника секретный канал связи для обмена ключами (рисунок 10). Создать такой канал связи вполне реально, поскольку нагрузка на него, вообще говоря, небольшая. Отметим теперь, что не существует единого шифра, подходящего для всех случаев.

Выбор вида шифра и его параметров (сложности, времени использования, времени актуальности, типов преобразований информации) существенно зависит от характера защищаемых секретов или тайны.

Рисунок 10 – Канал связи с использованием ключей

Некоторые тайны (например, государственные, военные и другие) должны сохраняться десятилетиями, а некоторые (например, биржевые) - уже через несколько часов можно разгласить.

Необходимо учитывать также и возможности того противника, от которого защищается данная информация. Одно дело - противостоять одиночке или даже банде уголовников, а другое дело - мощной государственной структуре.

Любая современная криптографическая система основана (построена) на использовании криптографических ключей. Она работает по определенной методологии (алгоритму, процедуре), состоящей из:

- одного или более алгоритмов шифрования (математических формул преобразования информации);
- ключей, используемых этими алгоритмами шифрования;
- системы управления ключами;
- незашифрованного текста;
- зашифрованного текста.

Симметричная (секретная) и асимметричная (открытая) методологии шифрования

Симметричная (секретная) криптосистема применяется достаточно широко для большинства коммерческих и финансово-экономических сообщений. В этой методологии и для шифрования, и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого они договорились до начала взаимодействия. Если ключ не был скомпрометирован (предан огласке и известен неопределенному кругу лиц), то при расшифровке автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, с помощью которого можно расшифровать информацию. Так как отправитель, так и получатель - единственные люди, которые знают этот симметричный ключ, при компрометации ключа будет скомпрометировано только взаимодействие этих двух пользователей.

Проблемой, которая будет актуальна и для других криптосистем, является вопрос о том, как безопасно распространять симметричные (секретные) ключи. Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных. Порядок использования систем с симметричными ключами:

1.Безопасно создается, распространяется и сохраняется симметричный секретный ключ.

2.Отправитель создает электронную подпись с помощью расчета хэш-функции для текста и присоединения полученной строки к тексту.

3.Отправитель использует быстрый симметричный алгоритм шифрования-расшифровки вместе с секретным симметричным ключом к полученному пакету (тексту вместе с присоединенной электронной подписью) для получения зашифрованного текста. Таким образом производится идентификация, так как только отправитель знает симметричный секретный ключ и может зашифровать этот пакет. Только получатель знает симметричный секретный ключ и может расшифровать этот пакет.

4.Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается по незащищенным каналам связи.

5.Получатель использует тот же самый симметричный алгоритм шифрования-расшифровки вместе с тем же самым симметричным ключом (который уже есть у получателя) к зашифрованному тексту для восстановления исходного текста и электронной подписи. Его успешное восстановление идентифицирует кого-то, кто знает секретный ключ.

6.Получатель отделяет электронную подпись от текста.

7.Получатель создает другую электронную подпись с помощью расчета хэш-функции для полученного текста.

8.Получатель сравнивает две этих электронных подписи для проверки целостности сообщения (отсутствия его искажения)

Другой подход использован при создании асимметричной (открытой) методологии шифрования. В этой методологии ключи для шифрования и расшифровки разные, хотя и создаются вместе. Один ключ делается известным всем, а другой держится в тайне. Данные, зашифрованные одним ключом, могут быть расшифрованы только другим ключом.

Все асимметричные криптосистемы являются объектом атак путем прямого перебора ключей, и поэтому в них должны использоваться гораздо более длинные ключи, чем те, которые используются в симметричных криптосистемах, для обеспечения эквивалентного уровня защиты. Это сразу же сказывается на вычислительных ресурсах, требуемых для шифрования, хотя алгоритмы шифрования на эллиптических кривых могут смягчить эту проблему.

В асимметричных криптосистемах важно, чтобы сеансовые и асимметричные ключи были сопоставимы в отношении уровня безопасности, который они обеспечивают. Если используется короткий сеансовый ключ (например, 40-битовый DES), то не имеет значения, насколько велики асимметричные ключи. Асимметричные открытые ключи уязвимы к атакам прямым перебором отчасти из-за того, что их тяжело заменить. Если атакующий узнает секретный асимметричный ключ, то будет скомпрометирован не только текущее, но и все последующие взаимодействия между отправителем и получателем.

Методика использования систем с асимметричными ключами для банковских и финансово-экономических пакетов состоит в следующем:

1.Разработчиком создаются и распространяются асимметричные открытые и секретные ключи. Секретный асимметричный ключ передается его владельцу. Открытый асимметричный ключ хранится в базе данных и администрируется центром выдачи сертификатов. Подразумевается, что пользователи должны верить, что в такой системе производится безопасное создание, распределение и администрирование ключами. Более того, если создатель ключей и лицо или система, администрирующие их, не одно и то же, то конечный пользователь должен верить, что создатель ключей на самом деле уничтожил их копию.

2.Создается электронная подпись текста с помощью вычисления его хэш-функции. Полученное значение шифруется с использованием

асимметричного секретного ключа отправителя, а затем полученная строка символов добавляется к передаваемому тексту (только отправитель может создать электронную подпись).

3.Создается секретный симметричный ключ, который будет использоваться для шифрования только этого сообщения или сеанса взаимодействия (сеансовый ключ), затем при помощи симметричного алгоритма шифрования/расшифровки и этого ключа шифруется исходный текст вместе с добавленной к нему электронной подписью - получается зашифрованный текст (шифр-текст).

4.Теперь нужно решить проблему с передачей сеансового ключа получателю сообщения. Отправитель должен иметь асимметричный открытый ключ центра выдачи сертификатов. Перехват незашифрованных запросов на получение этого открытого ключа является распространенной формой атаки. Может существовать целая система сертификатов, подтверждающих подлинность открытого ключа.

5.Отправитель запрашивает у центра сертификатов асимметричный открытый ключ получателя сообщения. Этот процесс уязвим к атаке, в ходе которой атакующий вмешивается во взаимодействие между отправителем и получателем и может модифицировать трафик, передаваемый между ними. Поэтому открытый асимметричный ключ получателя "подписывается" у центра сертификатов. Это означает, что центр сертификатов использовал свой асимметричный секретный ключ для шифрования асимметричного открытого ключа получателя. Только центр сертификатов знает асимметричный секретный ключ, поэтому есть гарантии того, что открытый асимметричный ключ получателя получен именно от него.

6.После получения асимметричный открытый ключ получателя расшифровывается с помощью асимметричного открытого ключа и алгоритма асимметричного шифрования/расшифровки. Естественно, предполагается, что центр сертификатов не был скомпрометирован. Если же

он оказывается скомпрометированным, то это выводит из строя всю сеть его пользователей. Поэтому можно и самому зашифровать открытые ключи других пользователей, (но где уверенность в том, что они не скомпрометированы).

7.Теперь шифруется сеансовый ключ с использованием асимметричного алгоритма шифрования-расшифровки и асимметричного ключа получателя (полученного от центра сертификатов и расшифрованного).

8.Зашифрованный сеансовый ключ присоединяется к зашифрованному тексту (который включает в себя также добавленную ранее электронную подпись).

9.Весь полученный пакет данных (зашифрованный текст, в который входит помимо исходного текста его электронная подпись, и зашифрованный сеансовый ключ) передается получателю. Так как зашифрованный сеансовый ключ передается по незащищенной сети, он является очевидным объектом различных атак.

10.Получатель выделяет зашифрованный сеансовый ключ из полученного пакета.

11.Теперь получателю нужно решить проблему с расшифровкой сеансового ключа.

12.Получатель должен иметь асимметричный открытый ключ центра выдачи сертификатов.

13.Используя свой секретный асимметричный ключ и тот же самый асимметричный алгоритм шифрования, получатель расшифровывает сеансовый ключ.

14.Получатель применяет тот же самый симметричный алгоритм шифрования-расшифровки и расшифрованный симметричный (сеансовый) ключ к зашифрованному тексту и получает исходный текст вместе с электронной подписью.

15.Получатель отделяет электронную подпись от исходного текста.

16.Получатель запрашивает у центра сертификатов асимметричный открытый ключ отправителя.

17.Как только этот ключ получен, получатель расшифровывает его с помощью открытого ключа центр сертификатов и соответствующего асимметричного алгоритма шифрования-расшифровки.

18.Затем расшифровывается хэш-функция текста с использованием открытого ключа отправителя и асимметричного алгоритма шифрования-расшифровки, повторно вычисляется хэш-функция полученного исходного текста, две эти хэш-функции сравниваются для проверки того, что текст не был изменен.

Стойкостью шифра называют способность шифра противостоять всевозможным атакам на него называют.

Под атакой на шифр понимают попытку вскрытия этого шифра.

Понятие стойкости шифра является центральным для криптографии. Хотя качественно понять его довольно легко, но получение строгих доказуемых оценок стойкости для каждого конкретного шифра - проблема нерешенная. Это объясняется тем, что до сих пор нет необходимых для решения такой проблемы математических результатов. Поэтому стойкость конкретного шифра оценивается только путем всевозможных попыток его вскрытия и зависит от квалификации криптоаналитиков, атакующих шифр. Такую процедуру иногда называют проверкой стойкости.

Практическая работа №6

Реализация метода простой замены

Цель работы: создание программы шифрования и дешифрования текста с использованием метода простой замены.

Применяемое оборудование: ПК, методические указания по выполнению практических работ.

Дополнительные теоретические сведения:

Шифрование методом замены (подстановки) основано на алгебраической операции, называемой подстановкой. Подстановкой называется взаимно-однозначное отображение некоторого конечного множества M на себя. Число N элементов этого множества называется степенью подстановки. Природа множества M роли не играет, поэтому можно считать, что M = {1, 2, ..., N}.

Шифр простой замены – класс методов шифрования, которые сводятся к созданию по определенному алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста.

При моноалфавитной замене каждой букве алфавита открытого текста ставится в соответствие одна буква шифротекста из этого же алфавита, например, шифр "Атбаш".

ИТ	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
ШТ	_	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р
ИТ	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	
ШТ	П	О	Н	М	Л	К	Й	И	З	Ж	Е	Д	Г	В	Б	А	

Ход работы:

1. Программа должна поддерживать следующие функции:
   a. ввод ключа пользователя для латинского и русского алфавита
   b. генерацию случайного ключа
   c. шифрование открытого текста методом простой и вывод на экран результата

d. дешифрование введенного шифротекста по известному ключу

2. Программа должна поддерживать возможность сохранения в отдельные файлы ключа, шифротекста и открытого текста, а также загрузку их из файла.

3. Программа должна содержать проверку ключа на ошибки (дублирование символов, полный повтор алфавита).

4. Программа должна поддерживать генерацию ключа на основе шифров Цезаря и Атбаш.

5. Интерфейс с программой должен быть организован на основе меню, обязательной частью которого должно являться подменю «Справка» с командой «О программе». При выборе этой команды должна выдаваться информация об авторе программы и выданном индивидуальном задании. Интерфейс пользователя программы может также включать панель управления с дублирующими команды меню графическими кнопками и строку состояния.

Указания по составлению отчета: результат решения заданий покажите преподавателю.

Критерии оценки

Оценка	
Отлично	Задание выполнено без существенных ошибок
Хорошо	Задание выполнено, но допущена одна существенная ошибка, исправленная студентом при указании преподавателя на ошибку
Удовлетворительно	Задание выполнено с наличием одной существенной ошибки, исправленной с помощью преподавателя
Неудовлетворительно	Задание выполнено, но допущено две или более существенных ошибок.

Практическая работа №7

Реализация метода моноалфавитной замены

Цель работы: создание программы шифрования и дешифрования текста с использованием метода простой замены.

Применяемое оборудование: ПК, методические указания по выполнению практических работ.

Дополнительные теоретические сведения:

Шифрование методом замены (подстановки) основано на алгебраической операции, называемой подстановкой. Подстановкой называется взаимно-однозначное отображение некоторого конечного множества M на себя. Число N элементов этого множества называется степенью подстановки. Природа множества M роли не играет, поэтому можно считать, что M = {1, 2, ..., N}.

Шифр простой замены – класс методов шифрования, которые сводятся к созданию по определенному алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста.

Ход работы:

1. Программа должна поддерживать следующие функции:
   a. ввод ключа пользователя для латинского и русского алфавита
   b. генерацию случайного ключа
   c. шифрование открытого текста методом простой замены и вывод на экран результата
   d. дешифрование введенного шифротекста по известному ключу
2. Программа должна поддерживать возможность сохранения в отдельные файлы ключа, шифротекста и открытого текста, а также загрузку их из файла.
3. Программа должна содержать проверку ключа на ошибки (дублирование символов, полный повтор алфавита).

4. Интерфейс с программой должен быть организован на основе меню, обязательной частью которого должно являться подменю «Справка» с командой «О программе». При выборе этой команды должна выдаваться информация об авторе программы и выданном индивидуальном задании. Интерфейс пользователя программы может также включать панель управления с дублирующими команды меню графическими кнопками и строку состояния.

Указания по составлению отчета: созданную программу покажите преподавателю.

Критерии оценки

Оценка	
Отлично	Задание выполнено без существенных ошибок
Хорошо	Задание выполнено, но допущена одна существенная ошибка, исправленная студентом при указании преподавателя на ошибку
Удовлетворительно	Задание выполнено с наличием одной существенной ошибки, исправленной с помощью преподавателя
Неудовлетворительно	Задание выполнено, но допущено две или более существенных ошибок.

Практическая работа №8

Реализация методов гомофонической и полиалфавитной замен

Цель работы: создание программы шифрования и дешифрования текста с использованием методов гомофонической и полиафавитной замены.

Применяемое оборудование: ПК, методические указания по выполнению практических работ.

Дополнительные теоретические сведения:

Гомофоническая замена одному символу открытого текста ставит в соответствие несколько символов шифртекста. Этот метод применяется для искажения статистических свойств шифртекста.

Пример. Открытый текст: «замена».

Алфавит открытого текста	А	Б	...	Е	Ж	З	...	М	Н	...
Алфавит шифртекста	17	23		97	47	76		32	55	
	31	44		51	67	19		28	84	
	48	63		15	33	59		61	34	
Шифртекст: "76 17 32 97 55 31".										

Таким образом, при гомофонической замене каждая буква открытого текста заменяется по очереди цифрами соответствующего столбца.

Полиалфавитная подстановка использует несколько алфавитов шифртекста. Пусть используется k алфавитов. Тогда открытый текст X = X1X2...XkXk+1...X2kX2k+1... заменяется шифртекстом Y = F1(X1)F2(X2)...Fk(Xk)Fk+1(Xk+1)...F2k(X2k)F2k+1(X2k+1), где Fi(Xj) – символ шифртекста алфавита i для символа открытого текста Xj.

Ход работы:

1. Программа должна поддерживать следующие функции:
   a. выбор метода замены
   b. ввод алфавита шифртекста (с выбором количества алфавитов)
   c. генерацию случайного ключа
   d. шифрование открытого текста и вывод на экран результата
   e. дешифрование введенного шифротекста по известному ключу

2. Программа должна поддерживать возможность сохранения в отдельные файлы ключа, шифротекста и открытого текста, а также загрузку их из файла.

3. Программа должна содержать проверку ключа на ошибки (дублирование символов, полный повтор алфавита).

4. Интерфейс с программой должен быть организован на основе меню, обязательной частью которого должно являться подменю «Справка» с командой «О программе». При выборе этой команды должна выдаваться информация об авторе программы и выданном индивидуальном задании. Интерфейс пользователя программы может также включать панель управления с дублирующими команды меню графическими кнопками и строку состояния.

Указания по составлению отчета: созданную программу покажите преподавателю.

Критерии оценки

Оценка	
Отлично	Задание выполнено без существенных ошибок
Хорошо	Задание выполнено, но допущена одна существенная ошибка, исправленная студентом при указании преподавателя на ошибку
Удовлетворительно	Задание выполнено с наличием одной существенной ошибки, исправленной с помощью преподавателя
Неудовлетворительно	Задание выполнено, но допущено две или более существенных ошибок.

Раздел 5. Организационно правовые методы информационной безопасности

Комплексная система защиты информации создается на объектах для блокирования (парирования) всех возможных или, по крайней мере, наиболее вероятных угроз безопасности информации. Для парирования той или иной угрозы используется определенная совокупность методов и средств защиты. Некоторые из них защищают информацию от нескольких угроз одновременно. Среди методов защиты имеются и универсальные методы, которые являются базовыми при построении любой системы защиты. Это, прежде всего, правовые методы защиты информации, которые служат основой легитимного построения и использования системы защиты любого назначения. Организационные методы защиты информации, как правило, используются для парирования нескольких угроз. Кроме того, организационные методы используются в любой системе защиты без исключений.

Государство должно обеспечить в стране защиту информации, как в масштабах всего государства, так и на уровне организаций и отдельных граждан. Для решения этой проблемы государство обязано:

1. выбрать государственную политику безопасности в области информационных технологий;
2. законодательно определить правовой статус компьютерных систем, информации, систем защиты информации, владельцев и пользователей информации и т.д.;
3. создать иерархическую структуру государственных органов, вырабатывающих и проводящих в жизнь политику безопасности информационных технологий;
4. создать систему стандартизации, лицензирования и сертификации в области защиты информации;
5. обеспечить приоритетное развитие отечественных защищенных информационных технологий;

6. повышать уровень образования граждан в области информационных технологий, воспитывать у них патриотизм и бдительность;

7. установить ответственность граждан за нарушения законодательства в области информационных технологий.

Очень важным правовым вопросом является установление юридического статуса компьютерных систем и особенно статуса информации, получаемой с применением компьютерных систем. Статус информации или ее правомочность служит основанием для выполнения (невыполнения) определенных действий. Например, в одних автоматизированных системах управления (АСУ) соответствующее должностное лицо имеет юридическое право принимать решения только на основании информации, полученной из АСУ. В других АСУ для принятия решения необходимо получить подтверждающую информацию по другим каналам. В одной и той же АСУ решение может приниматься как с получением подтверждающей информации, так и без нее. Примером может служить организация перевода денег с помощью АСУ. До определенной суммы перевод осуществляется автоматически при поступлении соответствующей заявки. Для перевода крупной суммы выполняются дополнительные процедуры проверки правомочности такой операции. Для этого может быть затребована дополнительная информация, в том числе и по дублирующей системе, а окончательное решение о переводе денег может принимать должностное лицо.

Правовой статус информации устанавливается с учетом ее стоимости (важности) и степени достоверности, которую способна обеспечить компьютерная система.

Важной составляющей правового регулирования в области информационных технологий является установление ответственности граждан за противоправные действия при работе с компьютерными системами или причинившие ущерб владельцам компьютерных систем,

получили название компьютерных преступлений. Согласно результатам совместного исследования Института компьютерной безопасности США и ФБР каждое компьютерное преступление наносит ущерб примерно в 200 тысяч долларов, и урон от компьютерных преступлений ежегодно растет в геометрической прогрессии.

В УК РФ в настоящее время глава 28 обозначает следующие преступления в сфере компьютерной безопасности:

- Неправомерный доступ к компьютерной информации (ст. 272);
- Создание, использование и распространение вредоносных компьютерных программ (ст. 273);
- Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274);
- Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1).

В каждой организации разрабатывается концепция информационной безопасности. Она является основным правовым документом, определяющим защищенность предприятия от внутренних и внешних угроз. Она определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в ИС. Концепция является методологической основой:

- формирования и проведения единой политики в области обеспечения безопасности информации в ИС;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и

организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

- координации деятельности структурных подразделений при проведении работ по созданию, развитию и эксплуатации ИС с соблюдением требований обеспечения безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ИС.

При разработке концепции должны учитываться основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно- программных средств защиты и противодействия угрозам безопасности информации, а также текущее состояние и перспективы развития информационных технологий.

Основные положения концепции должны базироваться на качественном осмыслении вопросов безопасности информации и не концентрировать внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

Положения концепции предусматривают существование в рамках проблемы обеспечения безопасности информации в ИС двух относительно самостоятельных направлений, объединенных единым замыслом: защита информации от утечки по техническим каналам и защита информации в ИС от несанкционированного доступа.

Система защиты информации (СЗИ), как и любая система, должна иметь определенные виды собственного обеспечения (совокупность обеспечивающих подсистем), опираясь на которые она будет выполнять свою целевую функцию. В частности, СЗИ может иметь:

1. **Правовое обеспечение**. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия.

2. **Организационное обеспечение**. Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами, такими как: служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая служба и другими.

3. **Аппаратное обеспечение**. Предполагается широкое использование технических средств, как для защиты информации, так и для обеспечения деятельности самой СЗИ.

4. **Информационное обеспечение**. Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности.

5. **Программное обеспечение**. К нему относятся различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей несанкционированного проникновения к источникам конфиденциальной информации.

6. **Математическое обеспечение**. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты.

7. **Лингвистическое обеспечение**. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации.

8. **Нормативно-методическое обеспечение**. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации.

Практическая работа №9

Анализ особенностей объекта защиты информации

Цель работы: анализ особенностей объекта защиты информации.

Ход работы:

1. Рассмотреть особенности различных типов носителей информации.

2. Отметить плюсы и минусы каждого типа носителей информации, условия хранения и обработки.

Указания по составлению отчета: отчет должен содержать название работы, цель работы, полученные результаты, ответы на контрольные вопросы и выводы.

Критерии оценки

Оценка	
Отлично	Задание выполнено без существенных ошибок
Хорошо	Задание выполнено, но допущена одна существенная ошибка, исправленная студентом при указании преподавателя на ошибку
Удовлетворительно	Задание выполнено с наличием одной существенной ошибки, исправленной с помощью преподавателя
Неудовлетворительно	Задание выполнено, но допущено две или более существенных ошибок.

Раздел 6. Роль стандартов в обеспечении информационной безопасности

Главная задача стандартов информационной безопасности — создать основу для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий. Каждая из этих групп имеет свои интересы и свои взгляды на проблему информационной безопасности.

Потребители, во-первых, заинтересованы в методике, позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки безопасности и, во-вторых, нуждаются в инструменте, с помощью которого они могли бы формулировать свои требования производителям. При этом потребителей (что вполне естественно) интересуют исключительно характеристики и свойства конечного продукта, а не методы и средства их достижения.

Производители также нуждаются в стандартах, как средстве сравнения возможностей своих продуктов, и в применении процедуры сертификации как механизме объективной оценки их свойств, а также в стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора. С точки зрения производителя требования должны быть максимально конкретными и регламентировать необходимость применения тех или иных средств, механизмов, алгоритмов и т. д. Кроме того, требования не должны противоречить существующим парадигмам обработки информации, архитектуре вычислительных систем и технологиям создания информационных продуктов. Этот подход также не может быть признан в качестве доминирующего, т. к. не учитывает нужд пользователей (а ведь это главная задача разработчика) и пытается подогнать требования защиты под существующие системы и технологии, а это далеко не всегда возможно осуществить без ущерба для безопасности.

Эксперты по квалификации и специалисты по сертификации рассматривают стандарты как инструмент, позволяющий им оценить уровень

безопасности, обеспечиваемый продуктами информационных технологий, и предоставить потребителям возможность сделать обоснованный выбор. Производители в результате квалификации уровня безопасности получают от объективную оценку возможностей своего продукта. Эксперты по квалификации находятся в двойственном положении: с одной стороны они как и производители заинтересованы в четких и простых критериях, над которыми не надо ломать голову как их применить к конкретному продукту (проще всего в виде анкеты с ответами типа да/нет), а с другой стороны, они должны дать обоснованный ответ пользователям — удовлетворяет продукт их нужды, или нет, ведь к конечном счете именно они принимают на себя ответственность за безопасность продукта, получившего квалификацию уровня безопасности и прошедшего сертификацию.

Таким образом, перед стандартами информационной безопасности стоит непростая задача — примирить эти три точки зрения и создать эффективный механизм взаимодействия всех сторон. Причем «ущемление» потребностей хотя бы одной из них приведет к невозможности взаимопонимания и взаимодействия и, следовательно, не позволит решить общую задачу — создание защищенной системы обработки информации. Необходимость в подобных стандартах была осознана уже достаточно давно (по меркам развития информационных технологий), и в этом направлении достигнут существенный прогресс, закрепленный в новом поколении документов разработки 90-годов. Наиболее значимыми стандартами информационной безопасности являются (в хронологическом порядке): «Критерии безопасности компьютерных систем министерства обороны США», Руководящие документы Гостехкомиссии России (только для нашей страны), «Европейские критерии безопасности информационных технологий», «Федеральные критерии безопасности информационных технологий США», «Канадские критерии безопасности компьютерных систем» и «Единые критерии безопасности информационных технологий».

Стандарт – это договоренность группы людей, организаций и т.д. Стандарт – не обязательно истина, но обязательно будет восприниматься всеми как эталон, а, следовательно, одинаково. Стандарт позволяет договориться о том, какие технологии, средства являются безопасными, а какие нет.

Стандарт должен:

1) Определить, что понимать под безопасностью и ввести концептуальную базу.

2) Выдвинуть набор требований к безопасной системе.

3) Предложить шкалу оценки безопасности, определенной в первой части стандарта.

Практическая работа №10

Составление регламента

Цель работы: получить навыки использования организационных мер защиты информационной безопасности

Ход работы:

1. Выделить уязвимости, которые можно устранить организационными и правовыми мерами защиты.

2. Определить стандарты, которыми следует руководствоваться при определении регламента безопасности.

2. Описать положения защиты информации для организации (правила и регламент работы с информацией).

Критерии оценки

Оценка	
Отлично	Задание выполнено без существенных ошибок
Хорошо	Задание выполнено, но допущена одна существенная ошибка, исправленная студентом при указании преподавателя на ошибку
Удовлетворительно	Задание выполнено с наличием одной существенной ошибки, исправленной с помощью преподавателя
Неудовлетворительно	Задание выполнено, но допущено две или более существенных ошибок.

Вопросы для промежуточного контроля

Тема 1. Введение в предмет. Угрозы информационной безопасности.

1. Что называется информационной безопасностью?

2. Какие данные называются критическими?

3. Какие вы знаете признаки компьютерных преступлений в интернет-технологиях и какие основные технологии, и методы используются при совершении компьютерных преступлений?

4. Какие четыре уровня защиты компьютерных (интернет технологий) и информационных ресурсов вы можете назвать?

5. Перечислите признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности?

Тема 2. Основные понятия теории информационной безопасности.

6. Перечислите меры защиты информационной безопасности.

7. Какие меры предпринимают по защите целостности информации?

8. Какие меры предпринимают по защите системных программ?

9. Дублирование информации и его классы.

10. Перечислите позиции административного уровня.

11. Назовите цель ОНРВ и его основные положения?

Тема 3. Программно-технические методы защиты.

12. Что такое межсетевой экран и какая у него роль в защите.

13. Законодательная основа информационной безопасности, статьи и пр.

14. Что такое политика безопасности на административном уровне?

15. Основные принципы защиты информации на административном уровне?

16. Средства Разграничения доступа.

17. Что такое CGI процедуры, их назначения?

18. Чем опасна программа, полученная из ненадежного источника, какие вы знаете средства контроля над такими программами?

19. Как осуществляется защита WEB-серверов?

Тема 4. Криптографические методы защиты.

20. Криптография и криптоанализ. Назначение криптографии.

21. Перечислите известные алгоритмы шифрования. Цифровые деньги и их характеристики.

22. Симметричная и асимметричная методология шифрования.

23. Криптографические средства защиты.

24. Квантовая криптография и ККС.

Тема 5. Организационно-правовые методы информационной безопасности.

25. Чем определяется концепция обеспечения безопасности АСОИ.

26. В чем состоит избирательная политика безопасности способом управления доступом.

27. Организационные меры безопасности АСОИ.

28. Матрица доступа в АСОИ.

29. Полномочное управление доступом.

30. Избирательное управление доступом.

Тема 6. Роль стандартов в обеспечении информационной безопасности.

31. Что такое универсальная операционная система?

32. Что такое компьютерный вирус.

33. Полиморфные вирусы.

34. Суррогатные платежные средства.

35. Файловые вирусы и алгоритм их работы.

36. Особенность макровирусов.

Список рекомендуемой литературы

1. Нестеров, С. А. Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва: Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — URL: https://biblio-online.ru/bcode/434171 (дата обращения: 02.12.2019).— Текст: электронный.
2. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — URL: https://biblio-online.ru/bcode/433715 (дата обращения: 02.12.2019).— Текст: электронный.
3. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / И. Н. Васильева. — Москва: Издательство Юрайт, 2019. — 349 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — URL: https://biblio-online.ru/bcode/433610 (дата обращения: 02.12.2019).— Текст: электронный.
4. Запечников, С. В. Криптографические методы защиты информации: учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва: Издательство Юрайт, 2019. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — URL: https://biblio-online.ru/bcode/433133 (дата обращения: 02.12.2019).— Текст: электронный.
5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — URL: https://biblio-online.ru/bcode/437163 (дата обращения: 02.12.2019).— Текст: электронный.

6. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — URL: https://biblio-online.ru/bcode/432966 (дата обращения: 02.12.2019).— Текст: электронный.
7. Правила оформления учебных работ студентов: учебно-метод. указ. / И. А. Жибинова, Е. А. Аракелян, О. В. Соколова, Ю. Н. Соина-Кутищева; под ред. И. А. Жибиновой. – Новокузнецк: НФИ КемГУ, 2018. – 1 CD-ROM. – Загл. с титул. диска. – ISBN 978-5-8353-2009-7. – Текст : электронный