Частное образовательное учреждение высшего образования

ЮЖНЫЙ УНИВЕРСИТЕТ

(ИУБиП)

И.Д АЛЕКПЕРОВ, В.В. ХРАМОВ, А.А. ГОРБАЧЕВА, Д.П. ФОМИЧЕВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В ЦИФРОВОЙ ЭКОНОМИКЕ: ЭЛЕМЕНТЫ ТЕОРИИ И ТЕСТОВЫЕ ЗАДАНИЯ

Учебное пособие

Утверждено
учебно-методическим советом университета

РОСТОВ-НА-ДОНУ

2020

УДК 681.3.067(07) + 06

Рецензенты: доктор физико-математических наук, профессор Л.В. Сахарова (РГЭУ);
кандидат технических наук, доцент Т.М. Линденбаум (РГУПС)

Алекперов И.Д.

Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И.Д. Алекперов, В.В. Храмов, А.А. Горбачева, Д.П. Фомичев; ЮУ (ИУБиП). – Ростов-на Дону, 2020. – 114 с.

Учебное пособие составлено согласно разделам Государственного образовательного стандарта для студентов направлений подготовки 38.03.01 «Экономика», 38.03.02 «Менеджмент», 38.03.03 «Управление персоналом» и 43.03.02 «Туризм».

Учебное пособие предназначено для специалистов в области автоматизированных систем цифровой экономике, аспирантов и студентов старших курсов академий «Экономика и управления» и «Цифрового развития».

Одобрено к изданию кафедрой «Информационные технологии и прикладная математика».

ОГЛАВЛЕНИЕ

1 ОБЩАЯ ПРОБЛЕМА БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЭКОНОМИЧЕСКИХ СИСТЕМАХ

1.1 Информация как объект и предмет защиты

Общие сведения

Объектом защиты информации является компьютерная (информационная) система или *автоматизированная система обработки информации* (АСОИ).

Информационная система – это организационно-упорядоченная совокупность информационных ресурсов, технических средств, технологий и персонала, реализующих информационные процессы в традиционном или автоматизированном режиме для удовлетворения информационных потребностей пользователей.

Информационная безопасность АСОИ – состояние рассматриваемой автоматизированной системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой стороны, ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Информационная безопасность достигается за счет соответствующей политики информационной безопасности.

Под *политикой информационной безопасности* понимают совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АСОИ от заданного множества угроз безопасности.

Система защиты информации – совокупность правовых норм, организационных мер и мероприятий, технических, программных и криптографических средств и методов, обеспечивающих защищенность информации в системе в соответствии с принятой политикой безопасности.

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

Конфиденциальность – обеспечение доступа к информации только авторизованным пользователям.

Целостность – обеспечение достоверности и полноты информации и методов ее обработки.

Доступность – обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Тестовые задания

1.1.1 Выбор. Какие из показателей характеризуют информацию как обеспечивающий ресурс:

важность;
полнота;
толерантность;
способ кодирования;
объем.

1.1.2 Выбор. Какие из показателей характеризуют информацию как обеспечивающий ресурс:

важность;
полнота;
адекватность;
самоорганизация;
целостность.

1.1.3 Ввод. <…> – свойство, позволяющее не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам.

1.1.4 Укажите правильный порядок уровней защиты для целостной модели:

1) охрана по периметру здания;
2) защита программных средств;
3) охрана по периметру территории объекта;
4) защита информации;
5) охрана помещения;
6) защита аппаратных средств.

1.1.5 Выбор. В проекте программного обеспечения (ПО) должен присутствовать специалист по информационной безопасности (ИБ), способный описать модели:

контроля доступа к объектам;
обеспечения конфиденциальности и целостности информации;
апеллируемости действий;
организации связей между программными модулями;
обращений к операционной системе (ОС) за системными ресурсами.

1.1.6 Выбор. В проекте ПО должен присутствовать специалист по ИБ, способный описать модели:

идентификации субъектов;
обеспечения конфиденциальности и целостности информации;
апеллируемости действий;
организации связей между программными модулями;
обращений к ОС за системными ресурсами.

1.1.7 Выбор. В проекте ПО должен присутствовать специалист по ИБ, способный описать модели:

идентификации субъектов;

аутентификации и авторизации;

контроля доступа к объектам;

организации связей между программными модулями;

обращений к ОС за системными ресурсами.

1.1.8 Ввод. <…> безопасности – это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

1.1.9 Ввод. Системы обнаружения … – устройства мониторинга активности в информационной среде, иногда с возможностью принятия самостоятельного участия в указанной активной деятельности.

1.1.10 Ввод. Сканер … – элемент системы обнаружения и предотвращения атак, устройство проверки качества безопасности информационной системы.

1.1.11 Выбор. Сканеры – это инструменты следующих категорий пользователей:

специалистов по безопасности, которые хотят проверить уровень уязвимости информационной системы (ИС) своей организации;

специалистов по сертификации информационных систем с точки зрения ИБ;

организаций, предоставляющих услуги по анализу защищенности ИС;

злоумышленников, использующих сканеры для поиска основы при реализации атаки;

администраторов локальных сетей;

«продвинутых» пользователей.

1.1.12 Ввод. <…> обеспечение – набор средств для обнаружения и уничтожения зловредного кода.

1.1.13 Ввод. <…> экраны – устройства контроля доступа из одной информационной сети в другую.

1.1.14 Ввод. <…> – устройства проверки качества функционирования модели безопасности для данной конкретной информационной системы.

1.1.15 Ввод. <…> – комплекс мероприятий, обеспечивающий для охраняемой информации конфиденциальность, целостность и доступность.

1.1.16 Ввод. <…> – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

1.1.17 Ввод. <…> – процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.

1.1.18 Ввод. <…> – защищаемые государством сведения в области его военной, внешнеполитической, экономической и оперативно-розыскной деятельности, распространение.

1.1.19 Ввод. <…> – соответствие эффективности защиты информации требованиям нормативных документов.

1.1.20 Ввод. Информационная <…> – приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных.

1.1.21 Ввод. <…> – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

1.1.22 Ввод. <…> – наименьшее разделяемое множество элементов, которые могут быть включены в профиль защиты или предмет безопасности.

1.1.23 Ввод. <…> – комплекс мероприятий, проводимых собственником информации для ограждения своих прав на владение и распоряжение информацией, создания условий, ограничивающих ее распространение и исключающих доступ к засекреченной информации и ее носителям.

1.1.24 Ввод. <…> – это несанкционированное изменение структуры компьютерной системы на этапах разработки и моделирования.

1.1.25 Выбор. По методу внедрения программных закладок в компьютерную систему бывают:

программно-аппаратные закладки;
загрузочные и драйверные закладки;
прикладные и исполняемые закладки;
закладки-имитаторы;
злонамеренные закладки.

1.1.26 Ввод. <…> – свойство системы выполнять возложенные на нее задачи в определенных условиях эксплуатации.

1.1.27 Ввод. <…> – свойство компьютерной системы сохранять работоспособность при отказах отдельных устройств, блоков, схем.

1.1.28 Ввод. <…> – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

1.1.29 Ввод. <…> – возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени.

1.1.30 Ввод. <…> безопасности – набор формальных правил, которые регламентируют функционирование механизма информационной безопасности.

1.2 Угрозы, уязвимости и риски информационной безопасности

Общие сведения

Под *угрозой* обычно понимают потенциально возможное событие, процесс или явление, которое может (воздействуя на что-либо) привести к нанесению ущерба чьим-либо интересам.

Угрозой интересам субъектов информационных отношений является потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

Нарушением безопасности является реализация угрозы безопасности.

В силу особенностей современных информационных систем, перечисленных выше, существует значительное число различных видов угроз безопасности субъектов информационных отношений.

Основными источниками угроз безопасности информационных систем и информации (угроз интересам субъектов информационных отношений) являются:

– стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.);

– сбои и отказы оборудования (технических средств) автоматизированной системы (АС);

– ошибки проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);

– ошибки в процессе эксплуатации (пользователей, операторов и другого персонала);

– преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Уязвимости представляют собой слабости защиты, ассоциированные с активами организации. Эти слабости могут использоваться одной или несколькими угрозами, являющимися причиной нежелательных инцидентов.

Уязвимость сама по себе не наносит ущерба, это только условие или набор условий, позволяющих угрозе причинить ущерб активам.

Другими словами, уязвимости – это любые факторы, делающие возможной успешную реализацию угроз. Следовательно, для оценки уязвимостей необходимо идентифицировать существующие механизмы безопасности и оценить их эффективность.

Идентификация уязвимостей должна определять связанные с активами слабости в следующих областях:

- физическом окружении;
- персонале, процедурах управления, администрирования и механизмах контроля;
- деловых операциях и предоставлении сервисов;
- технических средствах, программном обеспечении, телекоммуникационном оборудовании и поддерживающей инфраструктуре.

Угрозы и уязвимости должны объединиться для того, чтобы стать причиной инцидентов, которые могут причинить ущерб активам. Поэтому необходимо четко определять взаимосвязь между угрозами и уязвимостями.

Тестовые задания

1.2.1 Ввод. <…> безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными, и/или непреднамеренными воздействиями на нее.

1.2.2 Выбор. Методы защиты информации от случайных угроз включают в себя:

создание отказоустойчивых компьютерных систем (КС), минимизацию ущерба от стихийных бедствий;

оптимизацию взаимодействия человека с КС, блокирование ошибочных операций, дублирование информации, повышение надежности КС;

дублирование информации, повышение надежности КС, аудит, контроль целостности.

1.2.3 Выбор. Способы противоправного овладения информации включают в себя:

шпионаж;

диверсии;

использование вредительских программ и программных закладок;

несанкционированный доступ;

покупку алгоритмов и программных модулей;

исследование и разработку методов и программ формирования информационных массивов.

1.2.4 Выбор. Методы несанкционированного доступа к информации включают в себя:

физическое проникновение злоумышленника к источнику информации;

сотрудничество органа разведки или злоумышленника с работником конкурента;

дистанционный съем информации с носителя.

1.2.5 Выбор. Для добывания и уничтожения информации на объектах, не имеющих компьютерных систем, используются:

шпионаж;

диверсия;

троянские кони;

вирусы;

закладки.

1.2.6 Ввод. <…> – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

1.2.7 Ввод. Угрозы, не связанные с преднамеренными действиями злоумышленников и реализующиеся в случайные моменты времени, называют <…>.

1.2.8 Ввод. Под <…> безопасности информации понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

1.2.9 Выбор. Злоумышленником может быть:

разработчик КС;

сотрудник из числа обслуживающего персонала;

пользователь;

постороннее лицо;

программа-вирус;

программная закладка;

аппаратная закладка.

1.2.10 Выбор. Достоинства качественной модели рисков:

вычисления ускоряются и упрощаются;

нет необходимости присваивать денежную стоимость активу;

нет необходимости вычислять частоту проявления угрозы и точный размер ущерба;

не нужно вычислять соответствия эффективности предполагаемых мер угрозам;

повышается точность оценки;

уменьшается значение реального риска.

1.2.11 Ввод. <…> – вероятность реализации угрозы.

1.2.12 Ввод. Если риском является только возможное отрицательное воздействие угрозы, то <…> – ее действительное фактическое отрицательное воздействие.

1.2.13 Выбор. Информация в процессе ввода, хранения, обработки, ввода и передачи подвергается различным случайным воздействиям:

отказы и сбои аппаратуры;

помехи на линии связи от воздействий внешней среды;

ошибки человека как звена системы;

внедрение вирусов и программных закладок;

побочные наводки на вспомогательных и посторонних коммуникациях;

отходы обработки информации в виде бумажных и магнитных носителей.

1.2.14 Выбор. Информация в процессе ввода, хранения, обработки, ввода и передачи подвергается различным случайным воздействиям:

системные и системотехнические ошибки разработчиков;

структурные, алгоритмические и программные ошибки;

аварийные ситуации;

вирусные атаки из глобальных сетей;

побочное электромагнитное излучение аппаратуры системы;

побочные наводки по сети электропитания и заземления аппаратуры.

1.2.15 Ввод. <…> – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

1.2.16 Ввод. <…> реализации угрозы – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу информационного ресурса.

1.2.17 Ввод. <…> угрозы связаны с действиями человека, причинами которых могут быть определенное недовольство своей жизненной ситуацией, сугубо материальный интерес или простое развлечение для демонстрации своих способностей.

1.2.18 Выбор. К основным угрозам безопасности данных в вычислительных сетях относят:

раскрытие содержания передаваемых сообщений;

анализ трафика, позволяющий определить принадлежность отправителя и получателя данных к одной из групп пользователей сети, связанных общей задачей;

изменение потока сообщений, что может привести к нарушению режима работы какого-либо объекта, управляемого из удаленной ЭВМ;

неправомерное использование полномочий в системе разграничения доступа (СРД);

несанкционированное внедрение в информационную среду АРМ.

1.2.19 Выбор. К основным угрозам безопасности данных в вычислительных сетях относят:

изменение потока сообщений, что может привести к нарушению режима работы какого-либо объекта, управляемого из удаленной ЭВМ;

неправомерный отказ в предоставлении услуг;

несанкционированное установление соединения;

раскрытие информации о секретных ключах системы передачи данных;

неправомерный отказ от аутентификации.

1.3 Экономика информационной безопасности и инструменты оценки ее уровней

Общие сведения

Специалистам в области ИБ сегодня практически невозможно обойтись без знаний соответствующих стандартов и спецификаций. Для этого имеется несколько веских причин. Формальная причина состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и руководящим документам Федеральной службы по техническому и экспортному контролю) закреплена законодательно. Убедительны и содержательные причины. Во-первых, стандарты и спецификации – одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях ИБ и ИС. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными компаниями в области разработки ПО и безопасности программных средств. Во-вторых, и те, и другие являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов, причем в интернет-сообществе это средство работает весьма эффективно.

На верхнем уровне можно выделить две существенно отличающиеся друг от друга группы стандартов и спецификаций:

1) оценочные стандарты, предназначенные для оценки и классификации ИС и средств защиты по требованиям безопасности;

2) спецификации, регламентирующие различные аспекты реализации и использования средств и методов защиты.

Эти группы дополняют друг друга. Оценочные стандарты описывают важнейшие с точки зрения ИБ понятия и аспекты ИС, играя роль организационных и архитектурных спецификаций. Специализированные

стандарты и спецификации определяют, как именно строить ИС предписанной архитектуры и выполнять организационные требования.

«Общие критерии» содержат два основных вида требований безопасности:

1) функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям (сервисам) безопасности и реализующим их механизмам;

2) требования доверия, соответствующие пассивному аспекту; они предъявляются к технологии и процессу разработки и эксплуатации.

Тестовые задания

1.3.1 Ввод. Показатель <…> – характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.

1.3.2 Ввод. Для выбора модели построения защиты информации и оценки затрат на нее начальным условием является модель <…> нарушителя.

1.3.3 Ввод. С точки зрения модели потенциального нарушителя существует <…> класса безопасности.

1.3.4 Ввод. К <…> активам количественной модели рисков относятся средства обслуживания информационных технологий – аппаратное обеспечение, сетевое обеспечение, запасные части, документация и зарплата персонала для поддержания функционирования систем.

1.3.5 Ввод. Стоимость <…> активов должна учитывать два вида расходов: расходы на замену/восстановление программного обеспечения и данных, расходы при нарушении конфиденциальности/целостности/доступности.

1.3.6 Ввод. <…> актив – набор информации, который используется организацией в работе и может состоять из более мелких поднаборов.

1.3.7 Выбор. Программные средства, необходимые для полного анализа рисков и оценки затрат на их уменьшение, представляют собой инструмент для выполнения следующих операций:

построения модели ИС с позиции ИБ;
оценки ценности ресурсов;
составления списка угроз и уязвимостей, оценки их характеристик;
выбора контрмер и анализа их эффективности;
анализа вариантов построения защиты;
документирования (генерации отчетов);
оценки затрат злоумышленника на преодоление защиты.

1.3.8 Ввод. <…> – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, ПК).

1.3.9 Ввод. <…> ресурса – степень значимости ресурса для информационной системы, задаваемая в уровнях или в деньгах.

1.3.10 Ввод. Максимальное <…> время простоя – значение времени простоя, при котором ущерб, нанесенный организации наибольший.

2 ЗАЩИТА ИНФОРМАЦИИ ПРИ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ

2.1 Организационное обеспечение информационной безопасности

Общие сведения

Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявления внутренних и внешних угроз.

Организационная защита обеспечивает:

– организацию охраны, режима, работу с кадрами, документами;

– использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз безопасности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловлены не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

Организационные мероприятия – это мероприятия ограничительного характера, сводящиеся в основном к регламентации доступа и использования технических средств обработки информации. Они, как правило, проводятся силами самой организации путем использования простейших организационных мер.

К основным организационным мероприятиям можно отнести:

– организацию режима и охраны. Их цель – исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей;

– создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа;

– контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы;

– организацию и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.;

– организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

– организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение;

– организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

– организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;

– организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

В каждом конкретном случае организационные мероприятия имеют специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях:

– определение границ охраняемой зоны (территории);

– определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой территории;

– определение «опасных» с точки зрения возможности образования каналов утечки информации технических средств и конструктивных особенностей зданий и сооружений;

– выявление возможных путей проникновения злоумышленников к источникам конфиденциальной информации;

– реализация мер по обнаружению, выявлению и контролю за обеспечением защиты информации всеми доступными средствами.

Организационные мероприятия выражаются в тех или иных ограничительных мерах.

Можно выделить такие ограничительные меры, как территориальные, пространственные и временные.

Территориальные ограничения сводятся к умелому расположению источников на местности или в зданиях и помещениях, исключающих подслушивание переговоров или перехват сигналов радиоэлектронных средств.

Пространственные ограничения выражаются в выборе направлений излучения тех или иных сигналов в сторону наименьшей возможности их перехвата злоумышленниками.

Временные ограничения проявляются в сокращении до минимума времени работы технических средств, использовании скрытых методов связи, шифровании и других мерах защиты.

Одной из важнейших задач организационной деятельности является определение состояния технической безопасности объекта, его помещений,

подготовка и выполнение организационных мер, исключающих возможность неправомерного овладения конфиденциальной информацией, воспрещение ее разглашения, утечки и несанкционированного доступа к охраняемым секретам.

Специфической областью организационных мер является организация защиты ПЭВМ, информационных систем и сетей.

Одной из эффективных превентивных мер по обеспечению безопасности важных промышленных объектов является создание системы охраны от несанкционированного проникновения физических лиц – системы физической защиты (СФЗ).

Тестовые задания

2.1.1 Расположите по порядку уровни защиты для получения многоуровневой модели:

охрана по периметру территории объекта;
охрана по периметру здания;
охрана помещения;
защита аппаратных средств;
защита программных средств;
защита информации.

2.1.2 Выбор. Многоуровневой защитой участка контура называют защиту с <…> преградами:

параллельными;
перпендикулярными;
комбинированными;
сдублированными.

2.1.3 Ввод. <…> защиты – степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

2.1.4 Ввод. <…> методы защиты информации тесно связаны с правовым регулированием в области безопасности информации.

2.1.5 Ввод. <…> методы защиты информации – меры, мероприятия и действия должностных лиц для обеспечения заданного уровня безопасности информации.

2.1.6 Выбор. Подразделение конфиденциального делопроизводства включает в себя:

создание конфиденциальных документов;
обработку и хранение конфиденциальных документов;
контроль системы конфиденциального документооборота;
продажу конфиденциальных документов.

2.1.7 Ввод. Комплексная система защиты информации создается на объектах для <…> наиболее вероятных угроз безопасности информации.

2.1.8 Выбор. Участок защитного контура с параллельными преградами. Модель построена по принципу матрешек – это <…> модель:

двухфазная;
векторная;
многоуровневая;
многозвенная.

2.1.9 Ввод. <…> средства защиты – специальные организационно-технические и организационно-правовые мероприятия, акты и правила, осуществляемые в процессе создания и эксплуатации системы для организации и обеспечения защиты информации.

2.1.10 Выбор. Организационные мероприятия заключаются в следующем:
полное или частичное перекрытие каналов утечки информации;
объединение всех используемых средств защиты в целостный механизм;
профилактика нарушений политики безопасности;
внедрение новых мер по обеспечению ИБ.

2.2 Технологическое обеспечение информационной безопасности

Общие сведения

Широкое внедрение информационных технологий в жизнь современного общества привело к появлению ряда общих проблем информационной безопасности:

– необходимо гарантировать непрерывность и корректность функционирования важнейших информационных систем (ИС), обеспечивающих безопасность людей и экологической обстановки;

– необходимо обеспечивать защиту имущественных прав граждан, предприятий и государства в соответствии с требованиями гражданского, административного и хозяйственного права (включая защиту секретов и интеллектуальной собственности);

– необходимо защищать гражданские права и свободы, гарантированные действующим законодательством (включая право на доступ к информации).

Доступ к информации – ознакомление с информацией, ее обработка (в частности, копирование), модификация, уничтожение.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Объект доступа – единица информации автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Правила разграничения доступа – совокупность правил, регламентирующих права субъектов доступа к объектам доступа.

Санкционированный доступ – доступ к информации, который не нарушает правил разграничения доступа.

Несанкционированный доступ – доступ к информации, который нарушает правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

В связи с потенциальной уязвимостью ИС по отношению к случайным и предумышленным отрицательным воздействиям проблемы информационной безопасности перешли в разряд важнейших, стратегических, определяющих принципиальную возможность и эффективность применения ряда ИС в гражданских и военных отраслях.

Требования по обеспечению безопасности в различных ИС могут существенно отличаться, однако они всегда направлены на достижение трех основных целей:

– *целостность* – информация, на основе которой принимаются решения, должна быть достоверной и точной, защищенной от возможных непреднамеренных и злоумышленных искажений;

– *доступность* (готовность) – информация и соответствующие автоматизированные службы должны быть доступны, готовы к работе всегда, когда в них возникает необходимость;

– *конфиденциальность* – засекреченная информация должна быть доступна только тому, кому она предназначена.

Для решения проблем информационной безопасности необходимо сочетание законодательных, организационных, технологических и стандартизационных мероприятий.

Тестовые задания

2.2.1 Выбор. К основным функциям, выполняемым системой защиты операционной системы, относят:

разграничение доступа;

идентификацию и аутентификацию;

аудит;

управление политикой безопасности;

криптографические функции;

аутентификацию пользователя.

2.2.2 Выбор. Для защиты информации от несанкционированного доступа целенаправленно создается:

система разграничения доступа к информации;

система безопасности;

система аутентификации и идентификации.

2.2.3 Выбор. В КС нашли применение следующие подходы к организации разграничения доступа:

матричный;

полномочный (мандатный);

векторный.

2.2.4 Ввод. MAC (Mandatory access control) – это <…> управление доступом.

2.2.5 Выбор. Разграничение доступа бывает:

скрытое;

файловое;

избирательное;

полномочное.

2.2.6 Выбор. При разграничении доступа различают следующие операции с файлами:

копирование;

чтение;

выполнение программ;

удаление;

запись.

2.2.7 Ввод. В модели ACFM <…> – перечень пользователей, имеющих право доступа к объекту.

2.2.8 Ввод. <…> доступа – таблица, отображающая правила разграничения доступа.

2.2.9 Выбор. Метод доступа, согласно которому документу присваивается уровень конфиденциальности, а также могут присваиваться метки, отражающие категории конфиденциальности документа:

полномочный или мандатный метод;

матричный метод;

векторный метод.

2.2.10 Выбор. Система разграничения доступа (СРД) к информации должна содержать:

блок идентификации и аутентификации субъектов доступа, диспетчер доступа;

блок криптографического преобразования информации при ее хранении и передаче;

блок очистки памяти;

блок контроля целостности.

2.2.11 Выбор. Функциональные блоки системы разграничения доступа:

идентификации и аутентификации субъектов доступа;

антивирусный;

диспетчер доступа;

паролей.

2.2.12 Ввод. Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа, образуют <…> защиты.

2.2.13 Ввод. <…> возможности – функциональные возможности ПО, не описанные или не соответствующие технологии обработки информации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

2.2.14 Ввод. <…> выполнения функциональных объектов – определенная алгоритмом последовательность выполняемых функциональных объектов.

2.2.15 Ввод. <…> объект – элемент программы, содержащий фрагменты информации, циркулирующей в этой программе.

2.3 Техническое обеспечение информационной безопасности

Общие сведения

Все возможные способы защиты информации сводятся к нескольким основным методикам:

- воспрепятствование непосредственному проникновению к источнику информации с помощью инженерных конструкций технических средств охраны;
- скрытие достоверной информации;
- предоставление ложной информации.

Упрощенно принято выделять две формы восприятия информации – акустическую и зрительную (сигнальную). Акустическая информация в потоках сообщений носит преобладающий характер. Понятие зрительной информации весьма обширно, поэтому ее следует подразделять на объемно-видовую и аналогово-цифровую.

Самыми распространенными способами несанкционированного получения конфиденциальной информации являются:

– прослушивание помещений с помощью технических средств;

– наблюдение (в том числе фотографирование и видеосъемка);

– перехват информации с использованием средств радиомониторинга информативных побочных излучений технических средств;

– хищение носителей информации и производственных отходов;

– чтение остаточной информации в запоминающих устройствах системы после выполнения санкционированного запроса, копирование носителей информации;

– несанкционированное использование терминалов зарегистрированных пользователей с помощью хищения паролей;

– внесение изменений, дезинформация, физические и программные методы разрушения (уничтожения) информации.

Современная концепция защиты информации, циркулирующей в помещениях или технических системах коммерческого объекта, требует не периодического, а постоянного контроля в зоне расположения объекта. Защита информации включает в себя целый комплекс организационных и технических мер по обеспечению информационной безопасности техническими средствами. Она должна решать такие задачи, как:

– предотвращение доступа злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения;

– защита носителей информации от уничтожения в результате различных воздействий;

– предотвращение утечки информации по различным техническим каналам.

Способы и средства решения первых двух задач не отличаются от способов и средств защиты любых материальных ценностей, третья задача решается исключительно способами и средствами инженерно-технической защиты информации.

Тестовые задания

2.3.1 Выбор. Система связи, состоящая из передатчика (источника излучений), среды, в которой эти излучения распространяются, и приемника, посредством которой происходит утечка информации за счет побочных излучений, – это:

программный канал утечки информации;

канал шпионажа;

технический канал утечки информации.

2.3.2 Выбор. К основным группам технических средств ведения разведки относятся:

радиомикрофоны, электронные «уши», устройства перехвата телефонных сообщений;

устройства приема, записи, управления, видеосистемы наблюдения, записи и охраны;

системы определения местоположения контролируемого объекта;

системы контроля компьютеров и компьютерных сетей, системы сигнализации.

2.3.3 Выбор. Техническое обеспечение безопасности должно базироваться на:

системе стандартизации и унификации;

системе лицензирования деятельности;

системах сертификации средств защиты;

системе сертификации технических средств и объектов информатизации;

системе аттестации защищенных объектов информатизации;

системе аттестации сотрудников организации.

2.3.4 Выбор. Система физической защиты материальных объектов и финансовых ресурсов должна предусматривать:

систему инженерно-технических и организационных мер охраны;

систему регулирования доступа;

систему режима и контроля вероятных каналов утечки информации;

систему мер возврата материальных ценностей;

систему мер по обеспечению безопасности сотрудников.

2.3.5 Выбор. Система охранных мер должна предусматривать:

многорубежность построения охраны по нарастающей;

комплексное применение современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации;

надежное инженерно-техническое перекрытие вероятных путей несанкционированного вторжения в охраняемые пределы;

постоянное обновление и обслуживание технических средств защиты.

2.3.6 Выбор. Система охранных мер должна предусматривать:

устойчивую систему связи и управления всех взаимодействующих в охране структур;

высокую подготовку и готовность основных и резервных сил охраны к оперативному противодействию преступным действиям;

самоохрану персонала;

надежную систему технических средств физического противодействия нарушителям.

2.3.7 Выбор. Система регулирования доступа должна предусматривать:

объективное определение «надежности» лиц, допускаемых к работе;

максимальное ограничение количества лиц, допускаемых на объекты предприятия;

установление для каждого работника (или посетителя) дифференцированного по времени, месту и виду деятельности права доступа на объект;

четкое определение порядка выдачи разрешений и оформления документов для входа (въезда) на объект;

строго контролируемый доступ лиц в режимные зоны;

ограничение посещений режимных зон лицами, не участвующими в работе;

максимальное сокращение количества лиц, обладающих досмотровым иммунитетом.

2.3.8 Выбор. Система регулирования доступа должна предусматривать:

определение объемов контрольно-пропускных функций на каждом проходном пункте;

оборудование контрольно-пропускных пунктов техническими средствами, обеспечивающими достоверный контроль и объективную регистрацию проходящих;

высокую подготовленность и защищенность персонала контрольно-пропускных пунктов;

организацию тщательного контроля на каналах возможной утечки информации;

оперативное выявление причин тревожных ситуаций в режимных зонах;

пресечение их развития или ликвидацию во взаимодействии с силами охраны.

2.3.9 Выбор. В рамках технической политики обеспечения информационной безопасности необходимы:

реализация разрешительной системы допуска исполнителей к работам, документам и информации конфиденциального характера;

разграничение доступа пользователей к данным АС различного уровня и назначения;

учет документов, информационных массивов, регистрация действий пользователей ИС;

снижение уровня и информативности ПЭМИН;

тщательный отбор сотрудников, допущенных к работам, связанным с конфиденциальной информацией.

2.3.10 Выбор. В рамках технической политики обеспечения информационной безопасности необходимы:

снижение уровня акустических излучений;

активное зашумление в различных диапазонах;

противодействие оптическим и лазерным средствам наблюдения;

проверка технических средств и объектов информатизации на предмет выявления включенных в них закладных устройств («жучков»);

досмотр всех сотрудников, проходящих на охраняемую территорию.

2.4 Защита информации от несанкционированного доступа

Общие сведения

Получение доступа к ресурсам информационной системы предусматривает выполнение трех процедур: идентификация, аутентификация и авторизация.

Идентификация – присвоение пользователю (объекту или субъекту ресурсов) уникальных имен и кодов (идентификаторов).

Аутентификация – установление подлинности пользователя, представившего идентификатор, или проверка того, что лицо или устройство, сообщившее идентификатор, является действительно тем, за кого оно себя выдает. Наиболее распространенным способом аутентификации является присвоение пользователю пароля и хранение его в компьютере.

Авторизация – проверка полномочий или проверка права пользователя на доступ к конкретным ресурсам и выполнение определенных операций над ними.

Авторизация проводится с целью разграничения прав доступа к сетевым и компьютерным ресурсам.

Тестовые задания

2.4.1 Выбор. Получить несанкционированный доступ к информации при наличии системы разграничения доступа возможно только при:

сбоях, отказах КС;

наличии слабых мест в комплексной системе защиты информации;

это невозможно.

2.4.2 Ввод. <…> доступ – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники или автоматных систем.

2.4.3 Ввод. Под <…> разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

2.4.4 Выбор. Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

отсутствует СРД;

сбой или отказ в КС;

ошибочные действия пользователей или обслуживающего персонала КС;

ошибки в СРД;

фальсификация полномочий.

2.4.5 Ввод. Несанкционированное изменение структуры КС на этапах разработки и модернизации получило название <…>.

2.4.6 Ввод. Алгоритмические, программные и аппаратные <…> используются либо для непосредственного вредительского воздействия на КС, либо для обеспечения неконтролируемого входа в систему.

2.4.7 Выбор. Для вычислительных систем характерны следующие штатные каналы доступа к информации:

терминалы пользователей;

терминал администратора системы;

терминал оператора функционального контроля;

средства отображения информации;

средства исследования системы безопасности;

линии связи между аппаратными средствами данной вычислительной системы.

2.4.8 Выбор. Для вычислительных систем характерны следующие штатные каналы доступа к информации:

средства загрузки программного обеспечения;

средства документирования информации;

носители информации;

внешние каналы связи;

средства исследования парольной системы;

внутренний монтаж аппаратуры.

2.4.9 Выбор. Защита информационных ресурсов от несанкционированного доступа должна предусматривать:

обоснованность доступа, когда исполнитель должен иметь соответствующую форму допуска для ознакомления с информацией определенного уровня конфиденциальности;

персональную ответственность за сохранность доверенных пользователю информационных массивов, за свои действия в информационных системах;

надежность хранения, когда информационные массивы хранятся в условиях, исключающих несанкционированное ознакомление с ними, их уничтожение, подделку или искажение;

работу с кадрами и профилактику нарушений.

2.4.10 Выбор. Защита информационных ресурсов от несанкционированного доступа должна предусматривать:

разграничение информации по уровню конфиденциальности, а также предупреждение передачи конфиденциальной информации по незащищенным линиям связи;

контроль за действиями пользователей с документацией, а также в автоматизированных системах и системах связи;

очистку оперативной памяти, буферов при освобождении пользователем до перераспределения этих ресурсов между другими пользователями;

целостность технической и программной среды;

физическую защиту пользователей от злоумышленников.

2.4.11 Способ … используется для проверки целостности данных

Аутентификация

Шифрование

Резервная копия

Контрольная сумма

2.4.12 Кибервойна – это …

интернет-конфликт, связанный с проникновением в компьютерные системы и сети других стран.

серия оборудования персональной защиты, разработанного для солдат, участвующих в ядерной войне.

атака, совершаемая группой хакеров-любителей.

программа-симулятор для пилотов воздушных сил, которая позволяет им практиковаться в соответствии с моделированным военным сценарием.

2.4.13 Конфиденциальность информации еще называют …

Согласованность

Доверие

Точность

Неприкосновенность информации

2.4.14 Элементы … являются компонентами тройки CIA? (Выберите три варианта.)

Конфиденциальность

Доступность

Доступ

Масштабируемость

Целостность

Вмешательство

2.4.15 Примером «хактивизма» является …

Подросток взламывает веб-сервер местной газеты и публикует на нем картинку любимого героя мультфильма.

Преступники используют Интернет в попытках кражи денег из банков.

Одна страна пытается украсть военные тайны другой страны, проникнув в правительственные сети.

Группа защитников окружающей среды запускает атаку типа «Отказ в обслуживании» против нефтяной компании, ответственной за крупную утечку нефти.

2.4.16 Мотивация белого хакера – это …

Воспользоваться уязвимостью в личных неправомерных целях.

Выявление недостатков сетей и систем для повышения уровня безопасности этих систем.

Изучение операционных систем разных платформ для разработки новых систем.

Точная подстройка сетевых устройств с целью оптимизации их производительности и эффективности.

2.4.17 Способы, используемые для обеспечения конфиденциальности информации … (Выберите три варианта.)

Двухфакторная аутентификация

Настройки разрешения доступа к файлу

Резервная копия

Контроль версий

Шифрование данных

Идентификация по имени пользователя и паролю

2.4.18 Руткит предназначен для …

доставки рекламы без согласия пользователя

саморепликации независимо от других программ

маскировки в качестве легитимной программы

получения привилегированного доступа к устройствам без раскрытия себя

2.4.19 Характеристики описывающие программу-червь … (Выберите два варианта.)

выполняется при запуске ПО на компьютере

переходит на новые компьютеры без какого-либо вмешательства и без ведома пользователя

находится в неактивном состоянии, пока не понадобится злоумышленнику

является саморазмножающейся

заражает компьютеры, прикрепляясь к программному коду

2.4.20 Основная цель атак типа «отказ в обслуживании» (DoS-атак) – это …

упрощение доступа к внешним сетям

получение всех адресов в адресной книге на сервере

сканирование данных на целевом сервере

устранение способности целевой цели атаки обрабатывать другие запросы

2.4.21 Тип атаки … позволяет злоумышленнику воспользоваться методом подбора пароля (brute-force)
Взлом пароля
Отказ в обслуживании
Перехват пакетов
Социальная инженерия

2.4.22 Инструмент … используется для получения списка открытых портов на сетевых устройствах
Whois
Tracert
Ping
Nmap

2.4.23 Назовите основную цель отравления SEO (поисковой оптимизации).
Заставить обманным путем установить вредоносное ПО или раскрыть персональную информацию.
Создать ботнет из «зомби».
Переполнить сетевое устройство неправильно сформированными пакетами.
Увеличить веб-трафик на вредоносные сайты.

2.4.24 Технология, предотвращая слежение вредоносным ПО за активностью пользователей, сбор персональной информации и выдачу нежелательной всплывающей рекламы на компьютере пользователя?
Межсетевой экран
Антишпионское ПО
Двухфакторная аутентификация
Менеджер паролей

2.4.25 На общем компьютере скрыть личную историю просмотров в браузере от остальных сотрудников можно …
Использовать только шифрованное подключение для доступа к веб-сайтам.
Перезагрузить компьютер после закрытия веб-браузера.
Открывать веб-браузер в режиме конфиденциального просмотра.
Перемещать все загружаемые файлы в корзину.

2.4.26 Пользователю можно обезопасить себя от «подслушивания» сетевого трафика, когда он пользуется публичной точкой доступа Wi-Fi на своем ПК …
Отключить Bluetooth.

Использовать шифрование WPA2.
Подключаться через VPN-сервис.
Создать надежные и уникальные пароли.

2.4.27 Методом … можно лучше всего защитить данные хранящиеся на локальном жестком диске их от неавторизованного доступа
Шифрование данных
Удаление конфиденциальных файлов
Двухфакторная аутентификация
Дублированная копия жесткого диска

2.4.28 Пользователь должен проверить, что … прежде всего, подключаясь к публичной сети Wi-Fi в кафе?
на ноутбуке установлен основной пароль для защиты паролей, сохраненных в диспетчере паролей.
веб-браузер ноутбука работает в приватном режиме.
адаптер Bluetooth отключен.
ноутбук требует авторизации пользователя для обмена файлами и мультимедиа.

2.4.29 Технология … позволяет сократить издержки пользователя на оборудование и техническую поддержку системы резервного копирования данных?
Облачный сервис
Внешний жесткий диск
Сетевое хранилище
Лента

2.4.30 Устройства IoT представляют больше риска, чем другие вычислительные устройства в сети из-за того, что …
устройства IoT не могут функционировать в изолированной сети только с интернет-подключением.
большинство устройств IoT не требуют интернет-подключения и не могут получать новые обновления.
устройства IoT требуют незашифрованных беспроводных подключений.
большинство устройств IoT не получают регулярные обновления микропрограммного ПО.

2.4.31 Конфигурация беспроводного маршрутизатора … считается неадекватной защитой для беспроводной сети
Активация системы безопасности беспроводной сети
Использование шифрования WPA2
Предотвращение трансляции SSID
Изменение SSID и пароля беспроводного маршрутизатора, установленных по умолчанию

2.4.32 Надежнее всего можно предотвратить использование уязвимости в Bluetooth …

Использовать Bluetooth только для подключения к другому смартфону или планшету.

Использовать Bluetooth только при подключении к известному SSID.

Всегда отключать Bluetooth, когда он активно не используется.

Всегда использовать VPN при подключении с помощью Bluetooth.

2.4.33 Пароль … будет труднее всего взломать злоумышленнику?

super3secret2password1

mk$$cittykat104#

drninjaphd

10characters

2.4.34 Инструмент … может выполнять анализ трафика и портов в реальном времени, а также выявлять атаки сканирования портов, создания цифровых отпечатков и переполнения буфера

NetFlow

SIEM

Snort

Nmap

2.4.35 Инструмент … может выявлять вредоносный трафик, сравнивая содержимое пакета с известными сигнатурами атак

Nmap

IDS

NetFlow

Zenmap

2.4.36 Тип атаки … способен прерывать оказание услуг, переполняя сетевые устройства поддельным трафиком?

Сканирование портов

Метод грубой силы

DDoS

Атака нулевого дня

3 МАТЕМАТИЧЕСКИЕ И МЕТОДИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

3.1 Методы и модели обеспечения информационной безопасности

Общие сведения

Задача обеспечения информационной безопасности должна решаться системно. Это означает, что различные средства защиты (аппаратные, программные, физические, организационные и т.д.) должны применяться одновременно и под централизованным управлением. При этом компоненты системы должны «знать» о существовании друг друга, взаимодействовать и обеспечивать защиту как от внешних, так и от внутренних угроз. На сегодняшний день существует большой арсенал методов обеспечения информационной безопасности:

1) средства идентификации и аутентификации пользователей;
2) средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;
3) межсетевые экраны;
4) виртуальные частные сети;
5) средства контентной фильтрации;
6) инструменты проверки целостности содержимого дисков;
7) средства антивирусной защиты;
8) системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Системы шифрования позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам. Задача данного средства защиты – обеспечение конфиденциальности. Основные требования, предъявляемые к системам шифрования, – высокий уровень криптостойкости и легальность использования на территории России (или других государств).

Тестовые задания

3.1.1 Ввод. Критерии <…> – параметры, атрибуты, характеристики, на основе которых осуществляется разрешение или запрещение дальнейшей передачи данных в соответствии с заданными правилами разграничения доступа.

3.1.2 Выбор. Каждому объекту и субъекту присваивается определенный класс доступа в:

решетчатой модели безопасности;
модели Белла – Лападулы;
модели «Адепт 50»;

модели Кларка – Вильсона.

3.1.3 Выбор. Какой класс рекомендуется для защиты жизненно важной информации, утечка, разрушение или модификация которой могут привести к большим потерям для пользователя, если нарушитель-профессионал?

1-й класс;

2-й класс;

3-й класс;

5-й класс.

3.1.4 Ввод. «Отпечаток <…>» требует записи в каждую копию программы уникального идентификатора, присваиваемого конкретному покупателю программы, что позволяет отследить нарушителя авторского права.

3.1.5 Выбор. Ограничения, существующие в модели Белла – Лападулы:

запрет чтения информации субъектом с уровнем безопасности меньше, чем у объекта чтения;

запрет записи информации субъектом с уровнем безопасности больше, чем объект, в который записывается информация;

запрет чтения информации субъектом с уровнем безопасности больше, чем у объекта чтения;

запрет записи информации субъектом с уровнем безопасности меньше, чем объект, в который записывается информация.

3.1.6 Выбор. Модель, ориентированная на объекты (пользователи, терминалы, файлы и задания):

решетчатая модель безопасности;

модель Белла – Лападулы;

адепт 50;

модель Кларка – Вильсона.

3.1.7 Выбор. Модель, основанная на теории автоматов:

решетчатая модель безопасности;

модель Белла – Лападулы;

адепт 50;

модель Гогена – Мезигера.

3.1.8 Ввод. Использование «<…> знаков» основано на записи в код программы скрытой информации, позволяющей автору программы доказать то, что она является именно его интеллектуальной собственностью.

3.1.9 Выбор. Самое доступное решение, затрудняющее считывание скопированной информации:

нестандартная разметка (форматирование) носителя информации;

блокирование дисковых накопителей;

уничтожение дисковых накопителей;
блокирование копирования.

3.1.10 Выбор. В модели Кларка – Вильсона (1987) вводится понятие тройки, которая состоит из:
субъекта/программы/объекта;
субъекта/средства/программы;
модели/объекта/программы.

3.1.11 Выбор. Наиболее действенным методом противодействия несанкционированному выполнению скопированных программ является использование:
блока контроля среды размещения программы;
системы разграничения доступа;
парольной системы запуска программы.

3.1.12 Ввод. Выделяют два основных вида лицензий на программные продукты: временная и <…>.

3.1.13 Ввод. Выделяют два основных вида лицензий на программные продукты: <…> и оптимальная.

3.1.14 Ввод. <…> лицензия на программные продукты: позволяет использовать программные продукты неограниченному числу пользователей в течение ограниченного периода времени.

3.1.15 Ввод. <…> лицензия на программные продукты: позволяет использовать программные продукты ограниченному числу пользователей в течение неограниченного периода времени.

3.2 Криптографические методы защиты информации

Общие сведения

Наиболее эффективным средством повышения безопасности является криптографическое преобразование. Для того чтобы повысить безопасность, осуществляется одно из следующих действий:

1) передача данных в компьютерных сетях;
2) передача данных, которые хранятся в удаленных устройствах памяти;
3) передача информации при обмене между удаленными объектами.

Защита информации методом криптографического преобразования состоит в приведении ее к неявному виду через преобразование составных частей информации (букв, цифр, слогов, слов) с применением специальных алгоритмов либо аппаратных средств и кодов ключей. Ключ является

изменяемой частью криптографической системы, хранящейся в тайне и определяющей, какое шифрующее преобразование из возможных выполняется в данном случае.

Для изменения (шифрования) используется некоторый алгоритм или устройство, реализующее заданный алгоритм. Алгоритмы могут быть известны широкому кругу лиц. Управление процессом шифрования происходит с помощью периодически меняющегося кода ключа, который обеспечивает каждый раз оригинальное представление информации в случае применения одного и того же алгоритма или устройства. При известном ключе можно относительно быстро, просто и надежно расшифровать текст. Без знания ключа эта процедура может стать практически невыполнимой даже при использовании компьютера.

К методам криптографического преобразования предъявляются следующие необходимые требования:

1) ключ должен быть достаточно устойчивым к попыткам раскрытия исходного текста с помощью использования зашифрованного;

2) обмен ключа не должен быть сложным для запоминания;

3) затраты на защитные преобразования следует сделать приемлемыми при заданном уровне сохранности информации;

4) ошибки в шифровании не должны вызывать явную потерю информации;

5) размеры зашифрованного текста не должны превышать размеры исходного текста.

Методы, предназначенные для защитных преобразований, подразделяют на четыре основные группы: перестановки, замены (подстановки), аддитивные и комбинированные методы.

Методы перестановки и замены (подстановки) характеризуются коротким ключом, а надежность защиты определяется сложностью алгоритмов преобразования. Для аддитивных методов, наоборот, свойственны простые алгоритмы и длинные ключи. Комбинированные методы являются более надежными. Они чаще всего сочетают в себе достоинства используемых компонентов.

Вышеупомянутые четыре метода криптографического преобразования относятся к методам симметричного шифрования. Один ключ используется и для шифрования, и для дешифрования.

Основными методами криптографического преобразования являются методы перестановки и замены. Основа метода перестановки состоит в разбиении исходного текста на блоки, а затем в записи этих блоков и чтении зашифрованного текста по разным путям геометрической фигуры.

Симметричный вид шифров подразделяется на блочный и потоковый виды шифров. Отличительная особенность блочного вида шифров состоит в том, что они обрабатывают за одну итерацию сразу несколько байт (обычно по 8 или 16) открытой информации в отличие от потокового вида шифров, который обрабатывает по 1 байту (символу).

Шифрование методом замены заключается в том, что символы исходного текста (блока), записанные в одном алфавите, заменяются символами другого алфавита в соответствии с используемым ключом преобразования.

Комбинация этих методов привела к образованию метода производного шифра, который обладает сильными криптографическими возможностями. Алгоритм метода реализуется как аппаратно, так и программно, но рассчитан на реализацию с помощью электронных устройств специального назначения, что позволяет достичь высокой производительности и упрощенной организации обработки информации. Налаженное в некоторых странах Запада промышленное производство аппаратуры для криптографического шифрования позволяет резко увеличить уровень безопасности коммерческой информации при ее хранении и электронном обмене в компьютерных системах.

Тестовые задания

3.2.1 Ввод. <…> – шифр, в котором злоумышленнику полностью не известен алгоритм выполненного над сообщением преобразования, также его называют кодированием.

3.2.2 Выбор. В чем заключается принцип Киркхоффа в криптографии:

алгоритм преобразований должен быть широко известен и доступен каждому желающему;

ключ должен быть «зашит» в исходном алгоритме шифрования;

алгоритм шифрования должен базироваться на небольшом объеме секретной информации;

ключ, на основе которого производилось шифрование, должен быть известен только отправителю.

3.2.3 Выбор. При симметричном шифровании используются:

открытый ключ;

секретный ключ;

закрытый ключ;

это криптоалгоритм без ключа.

3.2.4 Выбор. Абсолютная стойкость шифра достигается, если:

размер ключа равняется размеру исходного текста;

размер ключа превышает размер исходного текста;

размер ключа меньше размера исходного текста;

размер ключа равняется или превышает размер исходного текста.

3.2.5 Ввод. Усложнение перестановки по <…> заключается в том, что для записи символов шифруемого текста используется специальная таблица, в которую введены усложняющие элементы.

3.2.6 Ввод. Атаки на шифры гаммирования основаны в большинстве своем либо на факте значительного отклонения статистических характеристик гаммы от действительно случайного потока, либо на <…> использовании некоторых частей гаммы в процессе шифрования.

3.2.7 Ввод. <…> шифрование – способ шифрования, при котором информация обрабатывается побитно.

3.2.8 Выбор. Поточное шифрование обрабатывает информацию:
побитно;
только строго определенного объема;
блоками по 32 бита;
блоками по 64 бита.

3.2.9 Выбор. Поточные шифры в зависимости от гаммы бывают:
с одноразовым или бесконечным ключом;
с конечным ключом;
на основе генератора псевдослучайных чисел;
одновременно с несколькими ключами.

3.2.10 Выбор. В шифрах гаммирования гамма – это:
бит исходного текста, подлежащего зашифровке;
бит текста, получившегося в результате шифрования из исходного;
бит шифрования, получающийся на каждом новом шаге автомата;
номер текущего шага шифрования.

3.2.11 Ввод. <…> шифрование представляет собой закон отображения множества входных блоков исходного текста на множество блоков зашифрованного текста, зависящий от секретного ключа.

3.2.12 Ввод. В <…> шифре единицей кодирования является один бит и результат кодирования не зависит от прошедшего ранее входного потока.

3.2.13 Ввод. При хороших статистических свойствах гаммы стойкость шифрования определяется только ее <…>.

3.2.14 Ввод. При <…> шифровании требуется по одному ключу для каждой пары пользователей.

3.2.15 Ввод. Основным препятствием к использованию ЛРС в качестве шифров является их неспособность противостоять атаке по <…> открытому тексту.

3.2.16 Ввод. Циклический сдвиг <…> – операция в блочном шифровании, обратимая к «циклическому сдвигу влево».

3.2.17 Ввод. <…> – операция в блочном шифровании, обратимая к «циклическому сдвигу вправо».

3.2.18 Выбор. Нелинейные поточные шифры включают в себя следующие классы алгоритмов:
комбинирующий;
сеть Файштеля;
фильтрующий;
динамический.

3.2.19 Ввод. <…> шифрование – способ шифрования, при котором обрабатывается информация только строго определенного объема.

3.2.20 Выбор. Обратимые операции в блочном шифровании:
И;
Исключающее ИЛИ;
ИЛИ;
НЕ.

3.2.21 Ввод. В <…> шифрах единицей кодирования является блок из нескольких байтов и результат кодирования зависит от всех исходных байтов этого блока.

3.2.22 Выбор. Какой алгоритм представляет собой сеть Файштеля из 16 раундов с добавлением входной и выходной перестановки бит?
ГОСТ 28147-89;
DES;
нелинейное поточное шифрование;
блочное шифрование.

3.2.23 Выбор. Какие из перечисленных операций выполняются в алгоритме DES?
перестановка бит/расширение блока с помощью повторов по определенной схеме;
наложение ключа раунда операцией XOR;
табличные подстановки;
перестановка бит.

3.2.24 Выбор. Алгоритм DES реализуется с помощью:
программы Diskreet;
платы «Криптон»;

специализированной микросхемы;
блюмингов.

3.2.25 Выбор. Причины ухода DES с рынка:
его удалось полностью взломать;
ориентированность на программную реализацию;
слишком малый размер ключа;
необходимость выполнять огромное количество битовых перестановок и выборок.

3.2.26 Ввод. Параметры алгоритма DES таковы: разрядность блока – 64 бита, размер ключа – <…> бит.

3.2.27 Ввод. Алгоритм DES представляет собой классическую сеть <…> из 16 раундов с добавлением входной и выходной перестановки бит.

3.2.28 Выбор. Какой известный алгоритм представляет собой сеть Файштеля из 32 раундов с двумя ветвями?
ГОСТ 28147-89;
DES;
пост-DES;
нелинейное поточное шифрование.

3.2.29 Выбор. Криптоалгоритм GOST был разработан спецслужбами:
США;
Советского Союза;
Канады;
Великобритании.

3.2.30 Выбор. От чего на 95 % зависит криптостойкость алгоритма ГОСТ 28147-89?
от размеров исходного блока данных;
от таблицы подстановок;
от ключа;
от работы процессора.

3.2.31 Выбор. Чем обусловлена большая устойчивость алгоритма ГОСТ к криптоатакам по сравнению с алгоритмом DES?
потенциальная емкость ключа в 256 бит;
зарекомендовавшая себя структура сети Файштеля;
взятое с «запасом» число раундов;
оптимизация под 32-разрядный процессор.

3.2.32 Выбор. Стандарт, введенный в действие 1 июля 1990 года, устанавливает единый алгоритм криптографического преобразования (шифрования) для отдельных компьютеров и вычислительных сетей:

ГОСТ 28147-89;
ГОСТ Р 50739-95;
ГОСТ Р 34.11-94;
ГОСТ Р 34.10-94;
ГОСТ Р 50922-96.

3.2.33 Ввод. Криптоалгоритм ГОСТ 28147-89 является единственным из официально опубликованных советских <…> шифров.

3.2.34 Ввод. Атака по времени исполнения криптоалгоритма основана на возможности злоумышленника замерять с очень высокой точностью <…> шифрования или дешифрования блока.

3.2.35 Ввод. Многочисленные виды атак на <…> основаны на предположении, что злоумышленник может каким-либо образом изменить один или несколько бит на различных этапах процесса шифрования.

3.2.36 Ввод. Атака класса дифференциальный криптоанализ впервые была опубликована Eli Biham и Adi Shamir в <…> году.

3.2.37 Ввод. Атака класса линейный криптоанализ впервые опубликована M. Matsui в <…> году.

3.2.38 Ввод. <…> шифрование – в этом методе для шифрования используется открытый ключ, а для дешифрования – закрытый.

3.2.39 Выбор. Практически стойким называется шифр, если:
единственный результативный метод атаки на него – полный перебор всех возможных ключей;
размер ключа равняется или превышает размер исходного текста;
не существует результативных методов атак на него;
размер ключа меньше размера исходного текста.

3.2.40 Выбор. При ассиметричном шифровании используются:
открытый ключ;
секретный ключ;
закрытый ключ;
это криптоалгоритм без ключа.

3.2.41 Ввод. <…> – для шифрования этим способом используется открытый ключ, а для дешифрования – закрытый.

3.2.42 Ввод. При <…> шифровании предполагается прежде всего программная реализация функций шифрования.

3.2.43 Ввод. Криптографическая система, в которой используется два ключа, секретный и открытый, причем ни один из ключей не может быть вычислен из другого за приемлемое время, называется криптосистемой с <…> ключом.

3.2.44 Ввод. <…> шифрование имеет следующую схему действия: получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным всем; отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю; получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

3.2.45 Выбор. Какое количество секретных ключей необходимо для асимметричного шифрования с участием N партнеров:

N;

2N;

N (N-)/2;

4N.

3.2.46 Выбор. К какой схеме в качестве множества исходных и зашифрованных сообщений используется кольцо вычетов Zm, где $m = p\ q$?

схема Рабина;

схема Вышнеградского;

схема Эль-Гамаля;

схема Райвеста – Шамира – Адлемана (RSA).

3.2.47 Ввод. В схеме RSA методом <…> решается в целых числах уравнение $e \times d + (p - 1) \times (q - 1) \times y = 1$.

3.2.48 Выбор. Теорема законности какого теста приведена ниже? Если тест выдает ответ «m – составное число», то m действительно является составным. Вероятность ответа «не знаю» для составного числа m не превосходит 1/4.

Рабина;

Вышнеградского;

Эль-Гамаля;

RSA.

3.2.49 Ввод. Схема Рабина похожа на алгоритм RSA, но возводит сообщение m в <…>.

3.2.50 Выбор. Какая схема асимметричного шифрования решает задачу дискретного логарифма?

схема на основе эллиптических кривых;

Диффи – Хеллмана;
RSA;
Эль-Гамаля.

3.2.51 Ввод. Асимметричная схема Эль-Гамаля предложена автором как логичное продолжение алгоритма обмена <…> Диффи – Хеллмана.

3.2.52 Ввод. Проблема дискретного логарифма состоит в том, что, зная основание степени и получившийся после возведения результат по модулю простого числа, невозможно за <…> время определить, в какую именно степень было возведено основание.

3.2.53 Ввод. <…> кривой, используемой в схеме Эль-Гамаля, является выражение вида $y2 = (x3 + a \times x + b) \bmod p$, где p – большое простое число.

3.2.54 Ввод. Схема Мак-Элиса основана на проблеме декодирования кода с <…> ошибок.

3.2.55 Ввод. Разрядность ключей раундов, применяемых в DES, равна <…> битам.

3.3 Электронная цифровая подпись

Общие сведения

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Закон об электронной цифровой подписи в Российской Федерации был издан 10 января 2002 года.

Средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Существует несколько схем построения цифровой подписи:

– На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифровывания его секретным ключом и передача его арбитру.

– На основе алгоритмов асимметричного шифрования. На данный момент такие схемы электронной подписи наиболее распространены и находят широкое применение.

Поскольку подписываемые документы переменного (и, как правило, достаточно большого) объёма, в схемах электронной подписи зачастую подпись ставится не на сам документ, а на его хэш. Для вычисления хэша используются криптографические хэш-функции, что гарантирует выявление изменений документа при проверке подписи. Хэш-функции не являются частью алгоритма электронной подписи, поэтому в схеме может быть использована любая надёжная хэш-функция.

Тестовые задания

3.3.1 Выбор. Электронная цифровая подпись решает следующие задачи:
обеспечение конфиденциальности послания;
аутентичность отправителя;
целостность сообщения;
не решает никаких важных задач.

3.3.2 Ввод. <…> – получается при использовании асимметричного шифрования наоборот, когда для шифрования применяется закрытый ключ, и служит для удостоверения личности отправителя.

3.3.3 Ввод. В цифровой подписи по схеме <…> отправитель выполняет над контрольной суммой такие действия, которые сделать может только он сам – извлечение квадратного корня в поле натуральных чисел $[0; n - 1]$.

3.3.4 Ввод. Проблема дискретного <…> – лежит в основе асимметричной схемы электронной цифровой подписи (ЭЦП) Эль-Гамаля.

3.3.5 Ввод. Стандарт США электронной цифровой подписи DSS, принятый в 1992 году, является одной из модификаций схемы <…>.

3.3.6 Выбор. Две самые распространенные схемы ЭЦП на данный момент в мире:

схема Рабина;

схема Вышнеградского;

схема Эль-Гамаля;

схема RSA.

3.3.7 Ввод. Алгоритм Государственного стандарта РФ по ЭЦП является переложением схемы Эль-Гамаля в область <…> кривых.

3.3.8 Ввод. ГОСТ Р 34.10-2001 – <…> Государственного стандарта РФ по ЭЦП.

3.3.9 Выбор. Хэш-функцией называется необратимое преобразование данных, обладающее следующими свойствами:

на вход алгоритма преобразования может поступать двоичный блок данных произвольной длины;

на выходе алгоритма получается двоичный блок данных фиксированной длины;

значения на выходе алгоритма распределяются по равномерному закону по всему диапазону возможных результатов;

при изменении хотя бы одного бита на входе алгоритма его выход значительно меняется: в идеальном случае инвертируется произвольная половина бит;

число бит в блоке не превышает 1 К;

исходным материалом не может быть текстовый файл.

3.3.10 Выбор. Хэш-функция называется криптографически стойкой, если она удовлетворяет следующим дополнительным требованиям:

зная результат хэш-функции, невозможно подобрать, кроме как полным перебором, какой-либо входной блок данных, дающий такое же значение на выходе;

невозможно подобрать, кроме как полным перебором, пару различных входных блоков, дающих на выходе произвольный, но одинаковый результат;

разрядность входа выше разрядности выхода;

разрядность выхода выше разрядности входа.

3.3.11 Ввод. Из теоремы, носящей название *парадокс дней рождения*, следует, что для того, чтобы создать одну коллизию для <…> -битной хэш-суммы, необходимо в среднем 264 документа.

3.3.12 Выбор. При проектировании хэш-функции по итеративной схеме возникают взаимосвязанные вопросы:

как поступать с данными, не кратными числу ($k - n$);

как добавлять в хэш-сумму длину документа, если это требуется;

как разбивать исходный текст на блоки;

как выбирать сжимающую функцию.

3.3.13 Ввод. Любой блочный шифр имеет два входа: открытый текст и ключ, а на выходе генерирует зашифрованный текст, таким образом, это идеальный претендент на ядро <…>.

3.3.14 Ввод. При организации ЭЦП по схеме <…> отправитель вычисляет и отправляет квадратный корень из контрольной суммы, на принимающей стороне остается только возвести ее в квадрат и проверить, совпало ли полученное значение с контрольной суммой подписанного ею документа.

3.3.15 Ввод. Алгоритм Государственного стандарта РФ по ЭЦП имеет полное название « <…> формирования и проверки электронной цифровой подписи».

3.4 Методология построения защищенных автоматизированных систем

Общие сведения

Актуальной является задача создания методики построения модели безопасности для синтеза настроек параметров безопасности автоматизированных систем защиты информации (АСЗИ) с целью уменьшения трудозатрат и повышения степени соответствия требованиям нормативных документов при проектировании систем (подсистем) ЗИ и планировании мер защиты.

Разрабатываемая методика построения модели безопасности АСЗИ должна обеспечить:

– значительное уменьшение трудозатрат с соблюдением соответствия требованиям нормативных документов при проектировании систем (подсистем) ЗИ и планировании мер защиты;

– исключение (уменьшение) ошибок проектирования систем (подсистем) ЗИ уже на ранних этапах проектирования за счет автоматизации синтеза настроек параметров безопасности АСЗИ;

– создание экспериментальной базы для последующей подготовки специалистов в области информационной безопасности.

Для решения этой задачи необходимо последовательно выполнить следующие действия:

1) определение формального механизма, адекватно выражающего заданную схему информационных потоков и правила управления ими;

2) построение модели безопасности, отражающей заданный порядок обработки информации, и формальное доказательство ее безопасности;
3) реализация системы обработки информации в соответствии с предложенной моделью;
4) доказательство адекватности допустимых в автоматизированной системе потоков информации, правил управления доступом к исходной схеме информационных потоков и правил управления ими.

Документы Гостехкомиссии РФ (ГТК) устанавливают девять классов защищенности АС от НСД, распределенных по трем группам. Каждый класс характеризуется определенной совокупностью требований к средствам защиты. В пределах каждой группы соблюдается иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается индексом NA, где N – номер группы (от 1 до 3). Следующий класс обозначается NБ и т.д.

Третья группа включает в себя АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает в себя АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и хранимой в АС на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа включает в себя многопользовательские АС, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности. Не все пользователи имеют равные права доступа. Группа содержит пять классов –1Д, 1Г, 1В, 1Б и 1А.

Тестовые задания

3.4.1 Выбор. Специфические угрозы информационной безопасности, возникающие при построении защиты БД:

абстрагирование;
агрегирование;
декомпозиция;
интерференция;
локализация;
комбинация разрешенных запросов для получения закрытых данных.

3.4.2 Выбор. К методам, осуществляющим противодействие угрозам при построении защиты БД, относятся:

блокировка ответа;
искажение ответа;
разделение БД;
случайный выбор записи;
контекстно-ориентированная защита;

контроль поступающих запросов.

3.4.3 Ввод. Правила <…> – перечень условий, по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных) и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций.

3.4.4 Выбор. К сетевым системам, тестируемым Intranet Scanner, относятся:
UNIX(r)-хосты;
операционные системы Microsoft Windows NT&153;, Windows(r) 95 и другие, поддерживающие стек протоколов TCP/IP;
интеллектуальные принтеры, имеющие IP-адрес;
X-терминалы.

3.4.5 Упорядочить по очередности основные этапы классификации АС:
разработка и анализ исходных данных;
выявление основных признаков АС, необходимых для классификации;
сравнение выявленных признаков АС с классифицируемыми;
присвоение АС соответствующего класса защиты информации от НСД.

3.4.6 Выбор. Необходимыми исходными данными для проведения классификации АС являются:
перечень защищаемых информационных ресурсов АС и уровень их конфиденциальности;
перечень лиц, имеющих доступ к штатным средствам АС, с указанием уровня их полномочий;
матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
режим обработки данных в АС;
перечень допустимых в АС программных средств;
матрица конфиденциальности объектов доступа.

3.4.7 Ввод. Выбор класса АС производится заказчиком и <…> с привлечением специалистов по защите информации.

3.4.8 Выбор. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:
наличие в АС информации различного уровня конфиденциальности;
уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
режим обработки данных в АС – коллективный или индивидуальный;
режим хранения информации на электронных носителях;
наличие информации о благонадежности сотрудников.

3.4.9 Ввод. Классы защищенности АС от НСД к информации подразделяются на <…> группы, отличающиеся особенностями обработки информации в АС.

3.4.10 Выбор. Третья группа защищенности от НСД к информации включает в себя АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности, и содержит классы:

3Г;
3В;
3Б;
3А.

3.4.11 Выбор. Вторая группа защищенности от НСД к информации включает в себя АС, в которых пользователи имеют одинаковые права доступа ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности, и содержит классы:

2А;
2Б;
2В;
2Г.

3.4.12 Выбор. Первая группа защищенности от НСД к информации включает в себя многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности, и содержит классы:

1Д;
1Г;
1В;
1Б;
1А.

3.4.13 Выбор. В общем случае комплекс решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД, условно состоящей из следующих подсистем:

управления доступом;
регистрации и учета;
криптографической;
обеспечения целостности;
обеспечения релевантности;
управления модификацией доступа.

3.4.14 Ввод. В подсистеме управления доступом должны осуществляться идентификация и проверка <…> субъектов доступа при входе в систему по паролю условно-постоянного действия.

3.4.15 Ввод. В подсистеме обеспечения целостности АС эта целостность проверяется при загрузке системы по наличию <…> компонентов СЗИ.

4 КОМПЬЮТЕРНЫЕ СРЕДСТВА РЕАЛИЗАЦИИ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

4.1 Программные закладки

Общие сведения

Программные закладки – класс программ с потенциально опасными последствиями, обязательно выполняющие следующие функции:

– разрушают код программы в памяти;

– сохраняют фрагменты информации из оперативной памяти в некоторой области внешней памяти прямого доступа;

– искажают произвольным образом, блокируют или подменяют выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ.

Изменения в функционировании, которые могут наблюдаться при работе программной закладки в системе, могут быть следующие:

1) снижение быстродействия вычислительной системы;

2) частичное или полное блокирование работы системы;

3) имитация физических (аппаратных) сбоев работы вычислительных средств и периферийных устройств;

4) переадресация сообщений;

5) обход программно-аппаратных средств криптографического преобразования информации;

6) обеспечение доступа в систему с несанкционированных устройств.

Программная реализация несанкционированного доступа к информации осуществляется на основе использования программных закладок. Под *несанкционированным доступом* (НСД) к ресурсам компьютерной системы понимают действия по использованию, изменению и уничтожению используемых данных указанной системы, производимые субъектом, не имеющим права на такие действия. Если компьютерная система содержит механизмы защиты от несанкционированного доступа, то несанкционированные действия могут быть вызваны:

– отключением или видоизменением защитных механизмов нелегальным пользователем;

– входом в систему под именем и с полномочиями реального пользователя.

В первом случае злоумышленник должен видоизменить программу, защитные механизмы в системе (например, отключить программу запросов пользователей), во втором – каким-либо образом выяснить или подделать идентификатор реального пользователя (например, подсмотреть или вычислить пароль, вводимый с клавиатуры).

В обоих случаях несанкционированный доступ можно представить моделью опосредованного доступа, когда проникновение в систему осуществляется на основе некоторого воздействия, произведенного

предварительно внедренной в систему программой или несколькими программами.

Тестовые задания

4.1.1 Выбор. Действия, выполняемые программными закладками:

внесение произвольных искажений в коды программ, находящихся в оперативной памяти компьютера;

удаление фрагментов информации из оперативной или внешней памяти;

искажение выводимой на внешние компьютерные устройства или в канал связи информации, полученной в результате работы других программ;

организация «зависаний» компьютера.

4.1.2 Ввод. <…> закладки – это закладки, ассоциированные с файлами, в которых содержится информация, необходимая операционной системе для управления подключенной к компьютеру периферией.

4.1.3 Выбор. Общей чертой программных закладок является:

перезапись файлов на диске С;

удаление всех программных файлов;

выполнение операции записи в операционную или внешнюю память;

самоуничтожение после активации.

4.1.4 Выбор. Что является общей чертой закладок?

перезапись файлов на диске С;

удаление всех программных файлов;

выполнение операции записи в операционную или внешнюю память;

самоуничтожение после активации.

4.1.5 Ввод. <…> закладки – преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

4.1.6 Выбор. Программная закладка реализует некоторую разрушающую функцию (или их совокупность):

искажение, подмена результатов функционирования программы;

нарушение функционирования программы;

уничтожение информации;

нелегитимный перехват, передача данных и сохранение фрагментов информации, обрабатываемых программой;

модификация кода программы;

выведение из строя компонентов ядра ЭВМ;

механическое повреждение периферийного оборудования.

4.1.7 Выбор. Программные закладки различают по:

способу доставки в систему;

специфике расположения;
отношению к программе-носителю;
длительности скрытого периода;
целевой эффективности;
языку программирования (написания);
взаимоотношениям с операционной системой.

4.1.8 Ввод. <…> программный элемент способен при определенных условиях вызвать модификацию программных или аппаратных объектов вычислительной системы и/или состояния вычислительной среды.

4.1.9 Ввод. Метрика <…> программного средства – измеряемая количественно характеристика разрушающих воздействий программного средства на объекты вычислительной системы.

4.1.10 Ввод. Уровень <…> программного средства считается максимальным в случае блокировки вычислительной средой выполнения хотя бы одной задачи, активизированной во время функционирования программного средства.

4.2 Вредительские программы

Общие сведения

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших общее название *вредительские программы*.

В зависимости от механизма действия вредительские программы делятся на четыре класса:

- логические бомбы;
- черви;
- троянские кони;
- компьютерные вирусы.

Логические бомбы – это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условий. Примерами таких условий могут быть: наступление заданной даты, переход КС в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

Червями называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, наконец, к блокировке системы.

Троянские кони – это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

Компьютерные вирусы – это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС.

Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

Тестовые задания

4.2.1 Выбор. Небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения в компьютерных системах, также могут выполнять изменение или уничтожение программного обеспечения или данных.

троянский конь;
программы-черви;
вирусы;
логические бомбы.

4.2.2 Выбор. Признаки внедренного кода программной закладки разделяют на следующие два класса:

качественные и визуальные;
обнаруживаемые средствами тестирования и диагностики;
резидентные и нерезидентные;
реальные и виртуальные;
качественные и визуальные;
обнаруживаемые средствами тестирования и диагностики;
резидентные и нерезидентные;
реальные и виртуальные.

4.2.3 Ввод. «<…> бомбы» – это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах и выполняемые только при соблюдении определенных условий.

4.2.4 Выбор. К явным проявлениям присутствия вируса можно отнести:

сбой аппаратных средств компьютерной системы;
замедление выполнения определенных действий;
звуковые эффекты;
уничтожение файлов и другие аналогичные действия.

4.2.5 Ввод. <…> – вредоносная программа, способная создавать свои копии или другие вредоносные программы и внедрять их в файлы, системные области компьютера, а также осуществлять иные деструктивные действия.

4.2.6 Выбор. Резидентные вирусы после их активации полностью или частично перемещаются из среды обитания:

в папку Program files;

на диск С;

в оперативную память ЭВМ;

в каждую работающую программу;

в сеть.

4.2.7 Выбор. Методы обнаружения вирусов включают в себя:

сканирование;

аналитический метод;

эвристический анализ;

виртуальный метод;

аппаратно-программные антивирусные средства.

4.2.8 Выбор. Что необходимо делать при работе с новыми съемными носителями и файлами?

запустить антивирусную программу;

записать на носитель антивирусную программу;

проверить на отсутствие загрузочных вирусов и файловых вирусов.

4.2.9 Выбор. Если не предполагается запись на магнитную дискету 3,5 дюйма, то необходимо:

в свойствах дискеты поставить метку «запрет записи»;

отформатировать дискету;

вытащить дискету и вставить заново;

открыть квадратное отверстие.

4.2.10 Выбор. К неявным проявлениям присутствия вируса можно отнести:

нарушение адресации;

сообщения антивирусных средств;

уничтожение файлов;

сбой устройств;

«зависание системы».

4.2.11 Выбор. Если заражение вирусом произошло, в первую очередь необходимо:

удалить файл с вирусом;

запустить программу AntiVirus;

выключить ЭВМ для уничтожения резидентных вирусов;

закрыть все папки и окна.

4.2.12 Ввод. <…> называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в сети и самовоспроизводить копии.

4.2.13 Ввод. <…> – это программы, полученные путем изменения или добавления команд в исходные программы, при последующем выполнении которых наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

4.2.14 Ввод. <…> система защиты информации охватывает весь жизненный цикл компьютерных систем от разработки до утилизации и всю технологическую цепочку сбора, хранения, обработки и выдачи.

4.3 Протоколы безопасности

Общие сведения

Протокол – это набор правил, определяющих взаимодействие абонентов сети и описывающих способ выполнения определённого класса функций. Говоря простым языком, протокол – совокупность правил, по которым компьютеры взаимодействуют между собой.

Криптографический протокол – это абстрактный или конкретный протокол, включающий в себя набор криптографических алгоритмов. В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах.

Классификация протоколов безопасности:

- протоколы шифрования/расшифровывания;
- протоколы электронной цифровой подписи (ЭЦП);
- протоколы идентификации/аутентификации;
- протоколы аутентифицированного распределения ключей.

Задачи протоколов безопасности:

- обеспечение различных режимов аутентификации;
- генерация, распределение и согласование криптографических ключей;
- защита взаимодействий участников;
- разделение ответственности между участниками.

Тестовые задания

4.3.1 Выбор. Наиболее важной задачей протоколов безопасности является:

абстрагирование;

инкапсуляция;

декомпозиция;

аутентификация;

локализация;

типизация.

4.3.2 Выбор. Инкапсулирование всех данных сетевого уровня, с выставлением новых заголовков и окончаний пакетов, называют:

шифрованием;

скрытием;

туннелированием;

защищенностью.

4.3.3 Выбор. Субъект, для которого требуется аутентификация, называется:

аутентификатором;

объектом;

кадром;

узлом;

модулем.

4.3.4 Выбор. Основные функции, выполняемые системой защиты операционной системы:

разграничение доступа;

идентификация и аутентификация;

аудит;

управление политикой безопасности;

криптографические функции;

сетевые функции.

4.3.5 Расположите в нужном порядке схему работы протокола PAP:

устанавливается PPP соединение;

субъект посылает аутентификационный запрос с указанием своего идентификатора и пароля;

объект проверяет полученные данные и подтверждает аутентификацию или отказывает в ней.

4.3.6 Выбор. За какое количество итераций происходит аутентификация в протоколе CHAP?

8;

5;

3;
7;
9.

4.3.7 Выбор. Процедура аутентификации в CHAP инициируется:
субъектом;
объектом;
совместно субъектом и объектом.

4.3.8 Выбор. В структуре EAP-пакета поле «Идентификатор»:
служит для обеспечения соответствия между запросом и ответом;
соответствует идентификатору запроса, на который посылается ответ;
соответствует запросу на предоставление данных для аутентификации;
все ответы верны.

4.3.9 Ввод. Криптографическим называется протокол, в основе которого лежит криптографический <…>.

4.3.10 Ввод. <…> – участник протокола, которому остальные участники полностью доверяют, предпринимая соответствующие действия для завершения очередного шага протокола.

4.4 Защита от обратного проектирования

Общие сведения

В большинстве случаев для обхода защиты взломщику требуется изучить принцип работы ее кода, и то, как она взаимодействует с самой защищаемой программой. Этот процесс изучения называется процессом реверсивной (обратной) инженерии. Данный процесс часто зависит от свойств человеческой психики, поэтому использование этих свойств позволяет снизить эффективность самого процесса реверсивной инженерии.

Обфускация (obfuscation – запутывание) – это один из методов защиты программного кода, который позволяет усложнить процесс реверсивной инженерии кода защищаемого программного продукта.

Обфускация может применяться не только для защиты ПП, она имеет более широкое применение, например, может быть использована создателями вирусов для защиты их творений и т.д.

Суть процесса обфускации заключается в том, чтобы запутать программный код и устранить большинство логических связей в нем, т.е. трансформировать его так, чтобы он был очень труден для изучения и модификации посторонними лицами (будь то взломщики или программисты,

которые собираются узнать уникальный алгоритм работы защищаемой программы).

Алгоритм обфускации в большинстве случаев рассматривается как алгоритм, которого должен придерживаться обфускатор (независимая программа, которая осуществляет процесс обфускации над переданным ей кодом).

На данный момент существуют различные алгоритмы осуществления процесса обфускации, начиная от общих (абстрактных) алгоритмов процесса обфускации и заканчивая более продвинутыми. Эти алгоритмы создавались в соответствии с возможностями того или иного языка программирования, и на сегодня большинство из них адаптировано непосредственно к языкам программирования высокого уровня. Ниже представлено короткое описание некоторых из них.

Алгоритм Колберга (Collberg`s algorithm)

Данный алгоритм оперирует следующими входными значениями:

- программа «A», состоящая из исходных или объектных (двоичных) файлов «{C1,C2}»;
- стандартные библиотеки, используемые программой «{L1,L2}»;
- набор трансформирующих процессов «T{T1,T2}»;
- определенный фрагмент кода «S», который извлекается из программы «A» и непосредственно будет подвержен трансформации;
- набор функций «E{E1,E2}», которые будут определять эффективность применения определенных трансформирующих процессов «{T1,T2}» к фрагменту кода «S»;
- набор функций «I{I1,I2}», которые будут определять важность фрагмента кода «S» и в зависимости от этого будут задавать определенное значение переменной «RequireObfuscation» (чем «S» важнее, тем эта переменная будет хранить большее значение);
- две числовые переменные «AcceptCost» > 0, «RequireObfuscation» > 0, где первое хранит информацию о доступном максимальном увеличении системных ресурсов, потребующихся программе «A», после того как она подвергнется обфускации, а вторая переменная будет хранить значение требуемого уровня осуществления обфускации (чем важнее фрагмент кода «S», тем это значение должно быть больше).

Алгоритм Колберга имеет такую последовательность операций:

1 Загрузка элементов «{C1,C2}» программы «A».

2 Загрузка библиотек «{L1,L2}».

3 Осуществление обфускации над программой «A» путем выделения фрагмента кода «S» и определения наиболее эффективного процесса трансформации для него. Этот этап повторяется до тех пор, пока не будет, достигнут требуемый уровень обфускации «RequireObfuscation» или допустимое увеличение ресурсов «AcceptCost».

4 Генерация трансформируемой программы «A».

Алгоритм Колберга считается общим алгоритмом осуществления процесса обфускации (т.е. он не определяет, как именно должен осуществляться тот или иной метод обфускации). Ниже будет рассмотрен более специализированный алгоритм, так как он описывает последовательность осуществления одного из методов обфускации, а именно обфускации управления.

Тестовые задания

4.4.1 Выбор. Алгоритм Колберга оперирует следующими входными значениями:

программа «A», состоящая из исходных или объектных файлов;

стандартные библиотеки, используемые программой;

набор преобразуемых процедур;

фрагмент кода, который извлекается из программы, будет подвержен трансформации.

4.4.2 Выбор. Алгоритм Колберга оперирует следующими входными значениями:

набор трансформирующих процессов;

фрагмент кода, который извлекается из программы, будет подвержен трансформации;

набор функций, которые выполняет исходная программа;

набор функций, которые будут определять важность фрагмента кода и задавать определенное значение переменной «RequireObfuscation».

4.4.3 Выбор. Алгоритм Колберга оперирует следующими входными значениями:

набор функций, которые будут определять важность фрагмента кода и задавать определенное значение переменной «RequireObfuscation»;

набор данных, предполагаемых к обработке исходной программой;

числовая переменная «AcceptCost» > 0, которая хранит информацию о доступном максимальном увеличении системных ресурсов, потребующихся исходной программе;

числовая переменная «RequireObfuscation» > 0, которая хранит значение требуемого уровня осуществления обфускации.

4.4.4 Выбор. Отметить правильные утверждения о процессе обфускации:

код программы в результате трансформации будет существенно отличаться от кода исходной программы, но при этом он будет выполнять те же функции и оставаться работоспособным;

процесс перепрограммирования займет больше времени, чем кодирование исходной программы;

при каждом процессе трансформации одного и того же кода исходной программы коды измененных программ будут различны.

4.4.5 Выбор. Отметить правильные утверждения о процессе обфускации:

код новой программы в результате трансформации будет отличаться от кода исходной программы языком программирования;

процесс реверсивной инженерии измененной программы будет более сложным, трудоемким и занимать больше времени, чем аналогичный процесс для исходной программы;

создание средства, детрансформирующего измененную программу в первоначальный вид, будет неэффективно.

4.4.6 Ввод. <…> – указывает на степень сложности осуществления реверсивной инженерии над кодом, прошедшим процесс обфускации.

4.4.7 Ввод. <…> – указывает на то, насколько хорошо данный процесс обфускации защитит программный код от применения деобфускаторов.

4.4.8 Ввод. <…> преобразования – позволяет оценить, насколько больше требуется системных ресурсов для выполнения кода, прошедшего процесс обфускации, чем для выполнения оригинального кода программы.

4.4.9 Укажите правильную последовательность операций в алгоритме Колберга:

1) загрузка элементов программы;

2) осуществление обфускации над программой путем выделения фрагмента кода и определения наиболее эффективного процесса трансформации для него;

3) загрузка библиотек;

4) генерация трансформируемой программы.

4.4.10 Укажите правильную последовательность операций в Chenxi Wang`s алгоритме:

1) приведение графа к однородному («плоскому») виду;

2) создание графа потока управления этой процедуры и его разбиение путем замены циклических конструкций в нем на конструкции типа «if (условие) goto»;

3) нумерация всех блоков в графе и добавление в код процедуры переменной (например, «swVar») хранящей номер следующего выполняемого блока.

4.4.11 Выбор. Лексическая обфускация включает в себя:

удаление всех комментариев в коде программ или изменение их на дезинформирующие;

изменение срока использования хранилищ данных – перехода от локального их использования к глобальному и наоборот;

удаление пробелов и отступов;

замену идентификаторов на произвольные длинные наборы символов, которые трудно воспринимать человеку;

добавление различных лишних операций;

изменение интерпретации данных определенного типа;

изменение расположения блоков программы так, чтобы это не повлияло на ее работоспособность.

4.4.12 Выбор. Лексическая обфускация включает в себя:

удаление всех комментариев в коде программы или изменение их на дезинформирующие;

удаление пробелов и отступов;

разделение переменных фиксированного диапазона на две и более переменных;

добавление различных лишних операций;

изменение срока использования хранилищ данных – перехода от локального их использования к глобальному и наоборот;

изменение расположения блоков программы так, чтобы это не повлияло на ее работоспособность.

4.4.13 Выбор. Лексическая обфускация включает в себя:

удаление всех комментариев в коде программы или замена их дезинформирующими;

удаление пробелов и отступов;

замену идентификаторов на произвольные длинные наборы символов, которые трудно воспринимать человеку;

изменение срока использования хранилищ данных – перехода от локального их использования к глобальному и наоборот;

добавление различных лишних операций;

изменение интерпретации данных определенного типа.

4.4.14 Выбор. Обфускацию данных принято делить на следующие группы:

обфускацию хранения;

обфускацию управления;

обфускацию соединения;

обфускацию переупорядочения.

4.4.15 Выбор. Обфускацию хранения реализуют за счет следующих методов:

добавление различных лишних операций;

изменение интерпретации данных определенного типа;

удаление всех комментариев в коде программы или замена их дезинформирующими;

замена идентификаторов на произвольные длинные наборы символов, которые трудно воспринимать человеку;

изменение расположения блоков программы так, чтобы это не повлияло на ее работоспособность;

разделение переменных фиксированного диапазона на две и более переменных.

4.4.16 Выбор. Обфускацию хранения реализуют за счет следующих методов:

изменение расположения блоков программы так, чтобы это не повлияло на ее работоспособность;

замена идентификаторов на произвольные длинные наборы символов, которые трудно воспринимать человеку;

изменение интерпретации данных определенного типа;

удаление всех комментариев в коде программы или замена их дезинформирующими;

разделение переменных фиксированного диапазона на две и более переменных.

4.4.17 Выбор. Обфускацию хранения реализуют за счет следующих методов:

удаление всех комментариев в коде программы или замена их дезинформирующими;

добавление различных лишних операций;

изменение срока использования хранилищ данных – перехода от локального их использования к глобальному и наоборот;

разделение переменных фиксированного диапазона на две и более переменных.

4.4.18 Выбор. Обфускация соединения включает в себя:

объединение переменных;

изменение расположения блоков программы так, чтобы это не повлияло на ее работоспособность;

изменение интерпретации данных определенного типа;

реструктурирование массивов;

изменение иерархий наследования классов.

4.4.19 Выбор. Обфускация соединения включает в себя:

объединение переменных;

изменение интерпретации данных определенного типа;

удаление всех комментариев в коде программы или замена их дезинформирующими;

реструктурирование массивов;

изменение иерархий наследования.

4.4.20 Выбор. Обфускация соединения включает в себя:

объединение переменных;

реструктурирование массивов;

замену идентификаторов на произвольные длинные наборы символов, которые трудно воспринимать человеку;

добавление различных лишних операций;

изменение иерархий наследования классов.

4.4.21 Выбор. Обфускация управления реализуется методами следующих групп:

обфускация вычислительная;

обфускация соединения;

обфускация последовательности;

обфускация переупорядочивания;

обфускация хранения.

4.4.22 Выбор. Обфускация управления реализуется методами следующих групп:

обфускация вычислительная;

обфускация соединения;

обфускация превентивная;

обфускация массивов;

обфускация пересылки.

4.4.23 Выбор. Обфускация управления реализуется методами следующих групп:

обфускация соединения;

обфускация последовательности;

обфускация превентивная;

обфускация лингвистическая;

обфускация данных.

4.4.24 Ввод. <…> обфускация предназначена для предотвращения применения злоумышленником деобфускаторов, декомпиляторов и остальных программных средств деобфускации.

4.4.25 Выбор. Аналитические методы оценки качества обфускации основаны на:

устойчивости;

эластичности;

стоимости преобразования;

эффективности;

квазимодальности.

5 ПРОГРАММА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ И ПУТИ ЕЕ РЕАЛИЗАЦИИ

5.1 Документы по информационной безопасности государства

Общие сведения

Государственная политика информационной безопасности РФ основана на положениях Конституции РФ о правах российских граждан и зафиксированы в законах РФ: «О безопасности»(от 28.12.2010 N 390-ФЗ), « Об информации, информационных технологиях и о защите информации»(от 27.07.2006 N 149-ФЗ), «О международном обмене информацией». Проблемам безопасности в информационной сфере посвящены Стратегия национальной безопасности РФ (Указ 31 декабря 2015 г. N 683), Доктрина информационной безопасности РФ, утвержденная президентом РФ В.В. Путиным (от 05.12.2016 года № 646)

Документ определяет национальные интересы России в информационной сфере, в том числе:

- обеспечение и защита прав и свобод граждан в части получения и использования информации, неприкосновенность частной жизни, а также сохранение духовно-нравственных ценностей;
- бесперебойное функционирование критической информационной инфраструктуры (КИИ);
- развитие в России отрасли ИТ и электронной промышленности;
- доведение до российской и международной общественности достоверной информации о государственной политике РФ;
- содействие международной информационной безопасности.

В Доктрине перечисляются основные информационные угрозы, стоящие перед страной и обществом:

1. Ряд западных стран наращивает возможности информационно-технического воздействия на информационную инфраструктуру в военных целях.
2. Усиливается деятельность организаций, осуществляющих техническую разведку в России.
3. Спецслужбы отдельных государств пытаются дестабилизировать внутриполитическую и социальную ситуацию в различных регионах мира. Цель — подрыв суверенитета и нарушение территориальной целостности государств. Методы — использование информационных технологий, а также религиозных, этнических и правозащитных организаций.
4. В зарубежных СМИ растет объем материалов, содержащих предвзятую оценку государственной политики России.

5. Российским журналистам за рубежом создаются препятствия, российские СМИ подвергаются «откровенной дискриминации».
6. Террористические и экстремистские группировки нагнетают межнациональную и социальную напряженность, занимаются пропагандой, привлекают новых сторонников.
7. Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере.
8. Растет число преступлений, связанных с нарушением конституционных прав и свобод человека, неприкосновенности частной жизни, защиты персональных данных. Эти преступления становятся все изощреннее.
9. Иностранные государства усиливают разведывательную деятельность в России. Растет количество компьютерных атак на объекты критической информационной инфраструктуры, их масштабы и сложность растут.
10. Высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий (электронная компонентная база, программное обеспечение, вычислительная техника, средства связи).
11. Низкий уровень эффективности российских научных исследований, направленных на создание перспективных информационных технологий. Отечественные разработки плохо внедряются, кадровый потенциал в этой области низкий.
12. Отдельные государства используют технологическое превосходство для доминирования в информационном пространстве. Управление интернетом на принципах справедливости и доверия между разными странами невозможно.

Документ называет основной стратегической целью обеспечения информационной безопасности в области обороны страны «защиту жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности».

Для России важно иметь сегодня современную концепцию вхождения в информационное общество. Она должна принципиально отличаться от концепций предыдущих периодов развития информатизации, которые были ориентированы в первую очередь на техническое обеспечение процессов информатизации. Теперь на первое место вышли вопросы социального характера, проблемы информационной безопасности.

Тестовые задания

5.1.1 Ввод. Государственная <…> – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

5.1.2 Ввод. <…> сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

5.1.3 Ввод. Система <…> государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

5.1.4 Ввод. <…> к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений.

5.1.5 Ввод. <…> к сведениям, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

5.1.6 Ввод. Гриф секретности – <…>, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и в сопроводительной документации на него.

5.1.7 Ввод. <…> сведений, составляющих государственную тайну, – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

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

5.1.9 Ввод. Средства защиты информации должны иметь <…>, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

5.1.10 Выбор. Допуск должностных лиц и граждан к государственной тайне предусматривает:

принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

письменное согласие на проведение в отношении них полномочными органами проверочных мероприятий;

ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

принятие на себя финансовых обязательств в рамках ответственности за разглашение;

добровольное ограничение в общении с гражданами других государств.

5.1.11 Ввод. Защите подлежит любая <…> информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

5.1.12 Ввод. Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью <…>, создают специальные службы, обеспечивающие защиту информации.

5.1.13 Ввод. <…> информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

5.1.14 Ввод. Собственник или владелец <…> информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации.

5.1.15 Ввод. <…>, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств.

5.1.16 Ввод. Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на <…> информации.

5.1.17 Ввод. Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-продажи, по другим формам обмена информационными ресурсами между организациями рассматриваются <…> судом.

5.1.18 Ввод. Отказ в доступе к <…> информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

5.1.19 Ввод. При <…> во время работы с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством.

5.1.20 Ввод. Для рассмотрения конфликтных ситуаций и защиты прав участников в сфере формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения могут создаваться временные и постоянные <…> суды.

5.1.21 Ввод. <…> интересы России – это совокупность сбалансированных интересов личности, общества и государства в экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других сферах.

5.1.22 Ввод. Национальные интересы России в <…> сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

5.1.23 Выбор. Важнейшими задачами обеспечения информационной безопасности РФ являются:

реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;

совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;

противодействие угрозе развязывания противоборства в информационной сфере;

получение права управления информационными ресурсами глобальной информационной сети.

5.1.24 Ввод. Под информационной безопасностью Российской Федерации понимается состояние защищенности ее <…> интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

5.1.25 Выбор. В целях обеспечения безопасности информационных систем (ИС) на территории России необходимо:

повысить безопасность ИС;

интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;

обеспечить защиту сведений, составляющих государственную тайну;

расширять международное сотрудничество Российской Федерации в области противодействия угрозе противоборства в информационной сфере;

отказаться от использования средств защиты информации иностранного производства.

5.1.26 Выбор. Угрозами информационному обеспечению государственной политики РФ могут являться:

монополизация информационного рынка России отечественными и зарубежными информационными структурами;

блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;

низкая эффективность информационного обеспечения государственной политики РФ;

преднамеренное противодействие чиновников и отдельных граждан национальным интересам РФ.

5.1.27 Выбор. К внешним источникам угроз информационной безопасности РФ относятся:

деятельность иностранных политических, экономических, военных и информационных структур, направленная против интересов РФ в информационной сфере;

стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве;

обострение международной конкуренции за обладание информационными технологиями и ресурсами;

увеличение технологического отрыва ведущих держав мира и их противодействие созданию конкурентоспособных российских информационных технологий;

усложнение структуры международного информационного пространства до неуправляемости.

5.1.28 Выбор. К внутренним источникам угроз информационной безопасности РФ относятся:

снижение степени защищенности законных интересов граждан, общества и государства в информационной сфере;

недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере;

недостаточное финансирование мероприятий по обеспечению ИБ РФ;

снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения ИБ;

отсутствие согласованной политики партий и групп в области ИБ.

5.1.29 Выбор. Основными мероприятиями по обеспечению ИБ РФ в сфере внутренней политики являются:

создание системы противодействия монополизации информационных услуг и СМИ;

активизация пропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России;

закрытие СМИ, создающих негативный образ жизни в РФ.

5.1.30 Выбор. Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики РФ;

распространение за рубежом дезинформации о внешней политике РФ;

нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

попытки несанкционированного доступа к информации и воздействия на информационные ресурсы РФ;

агрессивная информационная политика блока НАТО.

5.2 Обеспечение практической безопасности

Общие сведения

Сетевые и информационные технологии меняются настолько быстро, что статичные защитные механизмы, к которым относятся системы разграничения доступа, МЭ (межсетевые экраны), системы аутентификации во многих случаях не могут обеспечить эффективной защиты. Поэтому требуются динамические методы, позволяющие оперативно обнаруживать и предотвращать нарушения безопасности. Одной из технологий, позволяющей обнаруживать нарушения, которые не могут быть идентифицированы при помощи традиционных моделей контроля доступа, является технология обнаружения атак.

По существу, процесс обнаружения атак является процессом оценки подозрительных действий, которые происходят в корпоративной сети. Иначе говоря, *обнаружение атак* – это процесс идентификации и реагирования на подозрительную деятельность, направленную на вычислительные или сетевые ресурсы.

Система обнаружения вторжений (СОВ) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

Установлены пять классов защищенности МЭ. Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности – пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый – для 1Г, третий – 1В, второй – 1Б, самый высокий – первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.

Требования, предъявляемые к МЭ, не исключают требований, предъявляемых к средствам вычислительной техники (СВТ) и АС в соответствии с руководящими документами Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

При включении МЭ в АС определенного класса защищенности класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться.

Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5-го класса.

Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

– при обработке информации с грифом «секретно» – не ниже 3-го класса;

– при обработке информации с грифом «совершенно секретно» – не ниже 2-го класса;

– при обработке информации с грифом «особой важности» – не ниже 1-го класса.

Тестовые задания

5.2.1 Выбор. При работе в глобальной информационной сети самыми частыми и самыми опасными (с точки зрения размера ущерба) являются:

кражи;

подлоги;

непреднамеренные ошибки;

спамы.

5.2.2 Выбор. Обычно выделяют три основных вида угроз безопасности при работе в глобальной информационной сети – это:

угрозы раскрытия;

угроза целостности;

угроза отказа в обслуживании;

угроза HDT;

угроза блокировки.

5.2.3 Ввод. Системы обнаружения <…> – устройства мониторинга активности в информационной среде, иногда с возможностью принятия самостоятельного участия в указанной активной деятельности.

5.2.4 Ввод. <…> уязвимости – элемент системы обнаружения и предотвращения атак, устройство проверки качества безопасности информационной системы.

5.2.5 Выбор. Положительные стороны «Технологии сравнения с образцами» системы обнаружения атак:

наиболее простой метод обнаружения атак;

позволяет жестко увязать образец с атакой;

сообщение об атаке достоверно (если образец верно определен);

метод применим для всех протоколов;

для одной атаки создают всего несколько образцов;

если атака нестандартная, то она не мешает работе системы обнаружения атак.

5.2.6 Выбор. Отрицательные стороны «Технологии сравнения с образцами» системы обнаружения атак:

если образец определен слишком обще, то вероятен высокий процент ложных срабатываний;

если атака нестандартная, то она может быть пропущена;

для одной атаки, возможно, придется создавать несколько образцов;

метод ограничен анализом одного пакета и, как следствие, не улавливает тенденций и развития атаки;

слишком простой метод обнаружения атак;

жестко увязывает образец с атакой.

5.2.7 Выбор. Положительные стороны «Технологии соответствия состояния» системы обнаружения атак (СОА):

в применении метод лишь ненамного сложнее метода сравнения с образцами;

позволяет жестко увязать образец с атакой;

сообщение об атаке достоверно (если образец верно определен);

применим для всех протоколов;

уклонение от атаки более сложно (по сравнению с методом сравнения с образцами);

если образец определен в слишком общем виде, то это не выводит СОА из строя;

если атака нестандартная, то она может быть пропущена без ущерба для аппаратуры.

5.2.8 Выбор. Отрицательные стороны «Технологии соответствия состояния» СОА:

если образец определен в общем виде, то вероятен высокий процент ложных срабатываний;

если атака нестандартная, то она может быть пропущена;

в применении метод несколько сложнее метода сравнения с образцами;

жестко увязывает образец с атакой;

уклонение от атаки более сложно (по сравнению с методом сравнения с образцами).

5.2.9 Выбор. Положительные стороны анализа с расшифровкой протокола в системах обнаружения атак:

снижает вероятность ложных срабатываний, если протокол точно определен;

позволяет жестко увязать образец с атакой;

позволяет улавливать различные варианты на основе одной атаки;

позволяет обнаружить случаи нарушения правил работы с протоколами;

если стандарт протокола допускает неопределенности, то процент ложных срабатываний конечен;

метод сложен для перенастройки и не может быть изменен слабо подготовленными пользователями.

5.2.10 Выбор. Отрицательные стороны анализа с расшифровкой протокола в системах обнаружения атак:

жестко увязывает образец с атакой;

позволяет обнаружить случаи нарушения правил работы с протоколами;

если стандарт протокола допускает разночтения, то вероятен высокий процент ложных срабатываний;

метод сложен для настройки.

5.2.11 Ввод. «Технология сравнения с образцами» анализирует наличие в <…> некоторой фиксированной последовательности байтов – шаблона или сигнатуры.

5.2.12 Ввод. Технология соответствия состояния работает с <…> данных, а не с отдельным пакетом.

5.2.13 Ввод. <…> фильтр – это устройство, которое пропускает или отклоняет сетевые пакеты на основе предопределенных данных о сетевых (IP) адресах источника или получателя.

5.2.14 Ввод. МЭ с <…> соединения рассматривают каждый пакет в принадлежности его к конкретному соединению: кем, когда и как было инициировано соединение и какая активность была перед получением данного пакета.

5.2.15 Ввод. Технология посредника <…> заключается в том, что хосты во внутренней и во внешней сети устанавливают соединения между собой не напрямую, а через виртуального «посредника» – отдельный сервис или демон в МЭ, который общается с клиентом от имени сервера, а с сервером – от имени клиента.

5.2.16 Выбор. Недостатки персонального МЭ:

возможность влияния на функционирование МЭ со стороны пользователя ЭВМ;

более высокая стоимость владения: помимо закупочной цены необходимо учитывать стоимость распределенной поддержки;

меньшая защищенность от вирусных атак;

зависимость уровня защищенности от квалификации администратора сети.

5.2.17 Ввод. Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов при обработке информации с грифом «секретно» – не ниже <…> класса.

5.2.18 Ввод. Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов при обработке информации с грифом «совершенно секретно» – не ниже <…> класса.

5.2.19 Ввод. Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов при обработке информации с грифом «особой важности» – не ниже <…> класса.

5.2.20 Ввод. <…> экран – локальное или функционально распределенное программное-аппаратное средство, реализующее контроль за информацией, поступающей в автоматизированную систему.

5.2.21 Выбор. Укажите условия безопасности электронной почты:

текст сообщения должен быть доступен только отправителю и адресату;

неотрекаемость;

апеллируемость;

возможность отправить письмо, оставшись анонимным;

возможность бесплатно скачивать фильмы и музыку.

5.2.22 Выбор. Каковы основные действия для защиты от спама:

установить программу фильтр для E-mail;

периодически удалять ненужный вам «мусор» из почтового ящика;

написать жалобу провайдеру.

5.2.23 Ввод. Для защиты от мошенничества в Интернете следует никогда не осуществлять покупок через Интернет с использованием: кредитных <…> и никогда и не вводить каких-либо настоящих данных о себе.

5.2.24 Выбор. Специфические особенности решения задачи создания систем защиты информации (СЗИ):

неполнота и неопределенность исходной информации о составе ИС и характерных угрозах;

многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей СЗИ;

наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения СЗИ;

невозможность применения классических методов оптимизации;

высокая стоимость разработок компонентов СЗИ;

динамичное изменение критериев ИБ.

5.2.25 Выбор. Укажите правильную очередность этапов создания систем защиты информации:

определение информационных и технических ресурсов, а также объектов ИС, подлежащих защите;

выявление множества потенциально возможных угроз и каналов утечки информации;

проведение оценки уязвимости и рисков для ресурсов ИС;

определение требований к системе защиты информации;

осуществление выбора средств защиты информации и их характеристик;

внедрение и организация использования выбранных мер, способов и средств защиты;

осуществление контроля целостности и управление системой защиты.

5.2.26 Выбор. В МЭ должна обеспечиваться возможность регламентного тестирования:

реализации правил фильтрации;

процесса регистрации;

процесса идентификации и аутентификации администратора МЭ;

процесса контроля за целостностью программной и информационной части МЭ;

процедуры восстановления;

включения компьютера в работу.

5.2.27 Ввод. Межсетевой экран может строиться с помощью экранирующих <…>, которые обеспечивают установление соединения между

субъектом и объектом, а затем пересылают информацию, осуществляя контроль и/или регистрацию.

5.2.28 Ввод. <…> экран – это локальное или функционально-распределенное программное средство, реализующее контроль за информацией, поступающей в АС или выходящей из АС.

5.2.29 Ввод. <…> – функция МЭ, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области.

5.2.30 Ввод. Протоколы <…> уровня обеспечивают создание и функционирование логических каналов между программами в различных узлах сети, управляют потоками информации между портами, осуществляют компоновку пакетов о запросах и ответах.

6 НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1 Международные стандарты защиты информации

Общие сведения

Международные стандарты позволяют дополнить отечественное законодательство в тех областях, которые не затрагиваются российскими нормативно-правовыми документами. Примерами таких областей является аудит информационной безопасности, интеграция различных средств обеспечения безопасности, управление системами защиты и др. В отличие от положений российского законодательства требования международных стандартов носят рекомендательный характер.

«Оранжевая книга» была разработана в 1983 году. Этот документ был первым в области стандартов информационной безопасности. В «Оранжевой книге» сформулированы шесть базовых требований безопасности, которым должны соответствовать компьютерные системы, использующиеся для обработки конфиденциальной информации.

Требование 1. Политика безопасности.

Требование 2. Метки (степень конфиденциальности и/или режимы доступа).

Требование 3. Идентификация и аутентификация.

Требование 4. Регистрация и учет.

Требование 5. Контроль корректности функционирования средств защиты информации.

Требование 6. Непрерывность защиты.

Критерии определения безопасности компьютерных систем – стандарт Министерства обороны США, устанавливающий основные условия для оценки эффективности средств компьютерной безопасности, содержащихся в компьютерной системе. Критерии используются для определения, классификации и выбора компьютерных систем, предназначенных для обработки, хранения и поиска важной или секретной информации.

Классы безопасности компьютерных систем (TCSEC, Common Criteria)

Класс D. Минимальный уровень безопасности. В этот класс попадают системы, которые были заявлены на сертификацию, но ее не прошли. В настоящее время в данном классе не зарегистрирована ни одна ОС.

Класс C1. Избирательная защита доступа. Предусматривает наличие достоверной вычислительной базы (TCB), выполнение требований к избирательной безопасности. Обеспечивается отделение пользователей от данных (меры по предотвращению считывания или разрушения данных, возможность защиты приватных данных). В настоящее время по этому классу сертификация не предусмотрена.

Класс C2. Управляемая защита доступа. Системы данного класса способны осуществлять более точно выделенный контроль в плане избирательной защиты доступа. Действия пользователя связываются с

процедурами идентификации/аутентификации. Осуществляется наделение и лишение пользователей привилегий доступа. Кроме того, ведется аудит событий, критичных с точки зрения безопасности, выполняется изоляция ресурсов. По данному классу сертифицированы: AIX 4.3.1, OS/400 V4R4M0 with Feature Code 1920, AOS/VS II, Release 3.10, OpenVMS VAX and Alpha Version 6.1, CA-ACF2 MVS Release 6.1, NT Workstation и NT Server, Ver. 4.0, Guardian-90 w/Safeguard S00.01.

Класс B1. Маркированное обеспечение безопасности. В дополнение к требованиям класса C2 необходимо неформальное описание модели политики безопасности, маркировки данных, а также принудительного управления доступом к поименованным субъектам и объектам. По этому классу сертифицированы: CA-ACF2 MVS Release 6.1 в комплекте с CA-ACF2 MAC, UTS/MLS, Version 2.1.5+ (Amdahl), SEVMS VAX and Alpha Version 6.1, ULTRIX MLS+ Version 2.1 на платформе VAX Station 3100, CX/SX 6.2.1 (Harris Computer Systems), HP-UX BLS release 9.0.9+, Trusted IRIX/B release 4.0.5EPL, OS 1100/2200 Release SB4R7 (Unisys).

Класс B2. Структурированная защита. В этом классе систем TCB должна опираться на четко определенную и документированную формальную модель политики безопасности. Действие избирательного и принудительного управления доступом распространяется на все субъекты и объекты в системе. Выявляются тайные каналы (covert channel). TCB должна четко декомпозироваться на элементы, критичные и некритичные с точки зрения безопасности. Усиливаются механизмы аутентификации. Обеспечивается управление механизмами достоверности в виде поддержки функций системного администратора и оператора. Подразумевается наличие механизмов строгого управления конфигурацией. Система относительно устойчива к вторжению. По данному классу сертифицирована Trusted Xenix 4.0 (Trusted Information Systems).

Класс B3. Домены безопасности. TCB должна удовлетворять требованиям эталонного механизма мониторинга, который контролирует абсолютно весь доступ субъектов к объектам и при этом должен быть достаточно компактным, чтобы его можно было проанализировать и протестировать. Требуется наличие администратора по безопасности. Механизмы аудита расширяются до возможностей оповещения о событиях, критичных по отношению к безопасности. Требуются процедуры восстановления системы. Система крайне устойчива к вторжению. По данному классу сертифицирована XTS-300 STOP 5.2.E (Wang Government Services).

Класс A1. Верифицированное проектирование. Данный класс систем функционально эквивалентен классу B3 в том смысле, что не требуется добавления дополнительных архитектурных особенностей или не предъявляются иные требования к политике безопасности. Существенное отличие состоит в том, что для гарантии корректной реализации TCB требуется наличие формальной спецификации проектирования и соответствующих методов верификации. В данном классе не зарегистрирована ни одна ОС.

Рекомендации X.800 определяют функции (сервисы) безопасности, характерные для распределенных систем, уровни эталонной семиуровневой модели OSI, на которых могут быть реализованы функции безопасности, используемые механизмы безопасности, а также администрирование средств безопасности.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

- аутентификация;
- управление доступом;
- конфиденциальность данных;
- целостность данных;
- безотказность.

Рассматриваются три класса функциональных требований безопасности:

FAU – аудит безопасности;

FIA – идентификация/аутентификация;

FRU – использование ресурсов.

Тестовые задания

6.1.1 Выбор. Критерии оценки безопасности компьютерных систем МО США имеют название:

«Оранжевая книга»;

«Красная книга»;

«Желтая книга»;

TCSEC;

X800;

ITSEC.

6.1.2 Выбор. Критерии оценки безопасности информационных технологий (Европа) – это:

«Оранжевая книга»;

«Красная книга»;

«Желтая книга»;

TCSEC;

X800;

ITSEC.

6.1.3 Выбор. Канадские критерии безопасности компьютерных систем – это:

«Оранжевая книга»;

«Красная книга»;

CTCPEC;

TCSEC;

X800;

ITSEC.

6.1.4 Выбор. Требование целостности меток применимо к классам безопасности по TCSEC:

A1;
B3;
B2;
B1;
C2;
C1.

6.1.5 Выбор. Требование к гарантированности надежного восстановления применимо к классам безопасности по TCSEC:

B3;
B2;
B1;
C2;
C1.

6.1.6 Выбор. В соответствии с рекомендациями X.800 шифрование необходимо для:

аутентификации партнеров;
управления доступом;
конфиденциальности;
целостности соединения;
безотказности.

6.1.7 Выбор. В соответствии с рекомендациями X.800 электронная подпись необходима для:

аутентификации партнеров;
управления доступом;
конфиденциальности;
целостности соединения;
безотказности.

6.1.8 Выбор. В соответствии с рекомендациями X.800 управление маршрутизацией необходимо для:

аутентификации партнеров;
управления доступом;
конфиденциальности;
секретности трафика;
безотказности.

6.1.9 Выбор. В соответствии с рекомендациями X.800 нотаризация необходима для:

аутентификации партнеров;
управления доступом;
конфиденциальности;

целостности соединения;
безотказности.

6.1.10 Выбор. В соответствии с рекомендациями X.800 дополнение трафика необходимо для:
аутентификации партнеров;
управления доступом;
конфиденциальности;
целостности соединения;
безотказности.

6.1.11 Выбор. Разработанные Министерством обороны США критерии оценки уровня безопасности компьютерных систем получили название:
«Оранжевая книга»;
«Красная книга»;
стандарт CCITSE;
рекомендации X.800.

6.1.12 Выбор. Расширение «Оранжевой книги» для случаев использования компьютерных систем в информационной сети:
стандарт CCITSE;
рекомендации X.800;
«Красная книга».

6.1.13 Выбор. Вопросы классификации средств обработки информации рассматриваются:
в стандарте CCITSE;
«Оранжевой книге»;
«Красной книге».

6.1.14 Выбор. Согласно рекомендациям X.800 функции (сервисы) безопасности включают в себя:
аутентификацию, управление доступом, конфиденциальность данных, целостность данных, безотказность;
аутентификацию, управление доступом;
конфиденциальность данных, целостность данных, безотказность;
управление доступом, конфиденциальность данных, целостность КС, идентификацию.

6.1.15 Выбор. Любая операционная система, удовлетворяющая стандарту защищенности <…>, должна содержать подсистему защиты, выполняющую все основные функции защиты.
С2 «Оранжевой книги»;
Б2 «Оранжевой книги»;
Е3 «(ITSEC)»;
Е6 «(ITSEC)».

6.1.16 Выбор. Класс FAU – аудит безопасности включает в себя:

автоматическую реакцию в случае потенциального нарушения безопасности;

генерирование данных аудита;

неотрекаемость источника информации;

хранение событий аудита.

6.1.17 Выбор. Класс APE – оценка профиля защиты включает в себя:

среду безопасности;

политику управления доступом;

требования информационной безопасности;

заявки профиля защиты.

6.1.18 Выбор. Класс ACM – управление конфигурацией включает в себя:

автоматическое управление конфигурацией;

аудит процесса вычислений;

управление доступом;

область действия.

6.1.19 Выбор. Класс ADV – разработка включает в себя:

руководство администратора;

функциональную спецификацию;

соответствие представлений;

моделирование политики безопасности.

6.1.20 Выбор. Класс AVA – оценка уязвимости включает в себя:

анализ скрытых каналов;

злоупотребление;

функциональное тестирование;

средства и технологии.

6.1.21 Выбор. Класс FIA – идентификация и аутентификация включает в себя:

определение атрибутов пользователя;

спецификацию секретов;

привязку пользователя к субъекту;

устранение изъянов.

6.1.22 Выбор. Класс FMT – управление безопасностью включает в себя:

истечение атрибутов безопасности;

мониторинг результатов счета;

функциональное тестирование;

план поддержания уверенности.

6.1.23 Выбор. Класс EPR – сокрытие данных включает в себя:
анализ скрытых каналов;
анонимность;
разрыв связи;
неотслеживаемость.

6.1.24 Выбор. Класс FTA – доступ к предмету оценки включает в себя:
ограничение на объем атрибутов;
блокирование сессий;
семантическое тестирование;
историю доступа к объекту оценки.

6.1.25 Выбор. Класс FPT – защита системы включает в себя:
сбой безопасности;
злоупотребление;
обнаружение повтора;
разделение доменов.

6.1.26 Выбор. Вопросы классификации средств обработки информации рассматриваются:
в стандарте CCITSE;
«Оранжевой книге»;
«Красной книге».

6.1.27 Выбор. Базовые требования безопасности, отраженные в «Оранжевой книге», не включают в себя:
регистрацию и учет;
метки (степень конфиденциальности и/или режимы доступа);
защиту носителей информации;
политику безопасности.

6.1.28 Выбор. Базовые требования безопасности, отраженные в «Оранжевой книге», не включают в себя:
идентификацию и аутентификацию;
кадровую безопасность;
контроль корректности функционирования средств защиты информации;
непрерывность защиты.

6.1.29 Выбор. Базовые требования безопасности, отраженные в «Оранжевой книге», не включают в себя:
оценку рисков;
контроль корректности функционирования средств защиты информации;
идентификацию и аутентификацию;
метки (степень конфиденциальности и/или режимы доступа).

6.1.30 Выбор. Базовые требования безопасности, отраженные в «Оранжевой книге», не включают в себя:

непрерывность защиты;

политику безопасности;

регистрацию и учет;

мониторинг регуляторов безопасности.

6.2 Правовое регулирование отношений, связанных с информационными технологиями

Общие сведения

Уголовным кодексом Российской Федерации предусматривается ответственность в случае преднамеренного использования вредоносного программного обеспечения с целью:

– сбора или распространения сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия (статья 137);

– незаконного получения или разглашения сведений, составляющих коммерческую или банковскую тайну (статья 183);

– неправомерного доступа к охраняемой законом компьютерной информации (статья 272);

– нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (статья 274);

– нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, с использованием специальных технических средств, предназначенных для негласного получения информации (статья 138).

Уголовная ответственность распространяется также на лиц, совершивших действия по созданию, использованию и распространению вредоносных программ для ЭВМ (статья 273). При этом необходимо отметить, что в качестве вредоносного ПО могут выступать не только вирусы, программы типа «Троянский конь», но и программы, предназначенные для проведения информационных атак.

Регулирование отношений, связанных с созданием, правовой охраной, а также использованием программ для ЭВМ и баз данных, осуществляется при помощи законов «О правовой охране программ для электронных вычислительных машин и баз данных» и «Об авторском праве и смежных правах».

Тестовые задания

6.2.1 Ввод. Критерии <…> – это требования, используемые аккредитующим органом, которым должна отвечать организация, чтобы стать органом по сертификации.

6.2.2 Ввод. <…> защиты – это нормативный документ, который регламентирует все аспекты безопасности информационного продукта в виде требований к его проектированию, технологии, профилю защиты разработки и квалификационному анализу.

6.2.3 Ввод. Организационные методы защиты информации тесно связаны с <…> регулированием в области безопасности информации.

6.2.4 Выбор. Безопасность предприятия и защита информации в нем может быть реализована, в том числе и за счет:

обслуживания силами специальных организаций;

создания собственной службы безопасности;

законопослушания владельцев информации.

6.2.5 Выбор. Основными методами контроля со стороны государства за развитием отрасли информационных технологий являются:

стандартизация;

авторизация;

лицензирование;

шифрование.

6.2.6 Выбор. Регулирующими органами в сфере связи и информационных технологий являются:

Федеральная служба безопасности РФ;

Правительство РФ;

Федеральная служба охраны РФ;

Федеральная служба по техническому и экспортному контролю;

Верховный суд РФ;

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

6.2.7 Ввод. В соответствии с ФЗ «О связи» деятельность юридических лиц и индивидуальных предпринимателей по возмездному оказанию услуг связи осуществляется только на основании <…>.

6.2.8 Выбор. Статья 272 Уголовного кодекса РФ покрывает случаи:

неправомерного доступа к охраняемой законом компьютерной информации;

несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети;

создания, использования и распространения вредоносных компьютерных программ;

нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

6.2.9 Выбор. Статья 273 Уголовного кодекса РФ покрывает случаи:

неправомерного доступа к охраняемой законом компьютерной информации;

несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети;

создания, использования и распространения вредоносных компьютерных программ;

нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

6.2.10 Выбор. Статья 274 Уголовного кодекса РФ покрывает случаи:

неправомерного доступа к охраняемой законом компьютерной информации;

несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети;

создания, использования и распространения вредоносных компьютерных программ;

нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

6.2.11 Выбор. Согласно статье 272 УК РФ за неправомерный доступ к компьютерной информации грозит:

штраф до 200 тысяч рублей или лишение свободы до 2 лет;

штраф от 100 до 300 тысяч рублей или лишение свободы на срок до 4 лет;

лишение свободы на срок до 4 лет со штрафом до 200 тысяч рублей;

лишение свободы на срок до 5 лет со штрафом от 100 до 200 тысяч рублей;

лишение свободы на срок до 7 лет.

6.2.12 Выбор. Согласно статье 272 УК РФ за неправомерный доступ к компьютерной информации, причинивший крупный ущерб или совершенный из корыстной заинтересованности, грозит:

штраф до 200 тысяч рублей или лишение свободы до 2 лет;

штраф от 100 до 300 тысяч рублей или лишение свободы на срок до 4 лет;

лишение свободы на срок до 4 лет со штрафом до 200 тысяч рублей;

лишение свободы на срок до 5 лет со штрафом от 100 до 200 тысяч рублей;

лишение свободы на срок до 7 лет.

6.2.13 Выбор. Согласно статье 273 УК РФ за создание, использование и распространение вредоносных компьютерных программ грозит:

штраф до 200 тысяч рублей или лишение свободы до 2 лет;

штраф от 100 до 300 тысяч рублей или лишение свободы на срок до 4 лет;

лишение свободы на срок до 4 лет со штрафом до 200 тысяч рублей;

лишение свободы на срок до 5 лет со штрафом от 100 до 200 тысяч рублей;

лишение свободы на срок до 7 лет.

6.2.14 Выбор. Согласно статье 273 УК РФ за создание, использование и распространение вредоносных компьютерных программ, причинившие крупный ущерб или совершенные из корыстной заинтересованности, грозит:

штраф до 200 тысяч рублей или лишение свободы до 2 лет;

штраф от 100 до 300 тысяч рублей или лишение свободы на срок до 4 лет;

лишение свободы на срок до 4 лет со штрафом до 200 тысяч рублей;

лишение свободы на срок до 5 лет со штрафом от 100 до 200 тысяч рублей;

лишение свободы на срок до 7 лет.

6.2.15 Выбор. Согласно статьям 272 и 273 УК РФ за преступные деяния, если они повлекли тяжкие последствия или создали угрозу их наступления, грозит:

штраф до 200 тысяч рублей или лишение свободы до 2 лет;

штраф от 100 до 300 тысяч рублей или лишение свободы на срок до 4 лет;

лишение свободы на срок до 4 лет со штрафом до 200 тысяч рублей;

лишение свободы на срок до 5 лет со штрафом от 100 до 200 тысяч рублей;

лишение свободы на срок до 7 лет.

6.2.16 Выбор. Согласно статье 274 УК РФ за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей грозит:

штраф до 500 тысяч рублей или лишение свободы до 2 лет;

лишение свободы на срок до 4 лет со штрафом до 200 тысяч рублей;

лишение свободы на срок до 5 лет со штрафом от 100 до 200 тысяч рублей;

лишение свободы на срок до 7 лет.

6.2.17 Выбор. Варианты правового регулирования решения спорных ситуаций, связанных с использованием сети Интернет и находящихся под юрисдикцией разных государств и разных правовых систем:

по законодательству страны проживания пользователя;

по законодательству страны проживания собственника ресурса;

по законодательству страны проживания владельца;

по международным стандартам.

6.3 Государственная система обеспечения информационной безопасности в Российской Федерации

Общие сведения

Требования российского законодательства, определяющие обязательность защиты информации ограниченного доступа, изложены в федеральных законах и уточнены в документах Федеральной службы по техническому и экспортному контролю Российской Федерации (Гостехкомиссии России), ФСБ (ФАПСИ) и других государственных учреждений, имеющих отношение к обеспечению безопасности информации. Реализация и контроль этих требований осуществляются при помощи соответствующих государственных систем сертификации средств защиты и аттестации объектов автоматизации.

Правовую основу информационной безопасности обеспечивают: Конституция Российской Федерации, Гражданский и Уголовный кодекс, Федеральные законы «О безопасности» (№ 15-ФЗ от 07.03.2005), «О Государственной тайне» (№ 122-ФЗ от 22.08.2004), «Об информации, информатизации и защите информации» (№ 149-ФЗ от 27.07.2006), «Об участии в международном информационном обмене» (№ 85-ФЗ от 04.07.1996), «О коммерческой тайне» (№ 98-ФЗ от 29.07.2004), «О персональных данных» (№ 152-ФЗ от 27.07.2006), «О техническом регулировании» (№ 45-ФЗ от 09.05.2005), Доктрина информационной безопасности, указы Президента и другие нормативные правовые акты Российской Федерации.

Соблюдение правовых норм, установленных законодательными актами Российской Федерации, должно являться одним из основополагающих принципов при создании любой комплексной системы защиты от информационных атак.

Общие правовые основы обеспечения безопасности личности, общества и государства определены в Федеральном законе «О безопасности». Этим же законом определено понятие системы безопасности и ее функций, установлен порядок организации и финансирования органов обеспечения безопасности и правила контроля и надзора за законностью их деятельности.

Основные положения государственной политики в сфере обеспечения безопасности изложены в Доктрине информационной безопасности Российской Федерации.

В соответствии с Конституцией Российской Федерации (статьи 23, 24) мероприятия по защите данных от возможных информационных атак не должны нарушать тайну переписки, осуществлять сбор сведений о частной жизни сотрудников, а также ознакомление с их перепиской.

В Гражданском кодексе Российской Федерации (статья 139) определены характерные признаки информации, которая может составлять служебную или коммерческую тайну. Кроме того, в гражданском кодексе установлена

ответственность, которую несут лица за незаконные методы получения такой информации.

Вопросы отнесения информации к государственной тайне, а также порядок работы и защиты таких данных определены в Федеральном законе «О государственной тайне».

Федеральный закон № 184-ФЗ «О техническом регулировании» регулирует отношения, возникающие при разработке, принятии, применении и исполнении требований к процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации продукции, в том числе средств обнаружения атак. На основе данного закона в ближайшее время будет разработан технический регламент, который будет определять требования к информационной безопасности.

Тестовые задания

6.3.1 Ввод. В соответствии с законами и нормативными актами в министерствах, ведомствах, на предприятиях для защиты информации создаются специальные службы <…>.

6.3.2 Ввод. Соблюдение правовых <...>, установленных законодательными актами Российской Федерации, должно являться одним из основополагающих принципов при создании любой комплексной системы защиты от информационных атак.

6.3.3 Выбор. Общие правовые основы обеспечения безопасности личности, общества и государства, а также понятие системы безопасности и ее функций, порядок организации и финансирования органов обеспечения безопасности и правила контроля и надзора за законностью их деятельности определены в Федеральном законе:

«О безопасности»;

«О государственной тайне»;

«О персональных данных»;

«О коммерческой тайне».

6.3.4 Выбор. Характерные признаки информации, которая может составлять служебную или коммерческую тайну, а также установлена ответственность, которую несут лица за незаконные методы получения такой информации, определены в:

Трудовом кодексе Российской Федерации;

Гражданском кодексе Российской Федерации;

Уголовном кодексе Российской Федерации;

Уголовно-исполнительном кодексе Российской Федерации.

6.3.5 Выбор. Ответственность в случае преднамеренного использования вредоносного программного обеспечения предусматривается в:

Трудовом кодексе Российской Федерации;

Гражданском кодексе Российской Федерации;

Уголовном кодексе Российской Федерации;

Уголовно-исполнительном кодексе Российской Федерации.

6.3.6 Ввод. Уголовная ответственность распространяется также на лиц, совершивших действия по созданию, использованию и распространению <…> программ для ЭВМ (статья 273).

6.3.7 Выбор. Определяет понятие информационной безопасности и направлен на создание условий для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства Федеральный закон:

«Об информации, информатизации и защите информации»;

«Об участии в международном информационном обмене»;

«О безопасности»;

«О Государственной тайне».

6.3.8 Выбор. Отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления и предоставления потребителю документированной информации, регулируются Федеральным законом:

«О безопасности»;

«Об информации, информатизации и защите информации»;

«Об участии в международном информационном обмене»;

«О персональных данных».

6.3.9 Выбор. В соответствии с Указом Президента Российской Федерации № 188 от 06.03.1997 г. «Об утверждении перечня сведений конфиденциального характера» сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, составляют:

персональные данные;

служебную тайну;

коммерческую тайну;

информацию под грифом «секретно».

6.3.10 Выбор. В соответствии с Указом Президента Российской Федерации № 188 от 06.03.1997 г. «Об утверждении перечня сведений конфиденциального характера» служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами, составляют:

персональные данные;
служебную тайну;
коммерческую тайну;
информацию под грифом «секретно».

6.3.11 Выбор. В соответствии с Указом Президента Российской Федерации № 188 от 06.03.1997 г. «Об утверждении перечня сведений конфиденциального характера» сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами, составляют:

персональные данные;
служебную тайну;
коммерческую тайну;
информацию под грифом «секретно».

6.3.12 Выбор. Отношения, возникающие при разработке, принятии, применении и исполнении требований к процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации продукции, в том числе средств обнаружения атак, регулирует Федеральный закон:

«О техническом регулировании»;
«Об информации, информатизации и защите информации»;
«О безопасности»;
«О Государственной тайне».

Список использованных источников

1. Доктрина информационной безопасности РФ(от 05.12.2016 года № 646), URL: http://docs.cntd.ru/document/420384668 (Время обращения 12.12.2019г.)
2. Федеральный закон «О безопасности»(от 28.12.2010 N 390-ФЗ), URL: https://legalacts.ru/doc/federalnyi-zakon-ot-28122010-n-390-fz-o/(Время обращения 12.12.2019г.)
3. Федеральный закон « Об информации, информационных технологиях и о защите информации»(от 27.07.2006 N 149-ФЗ), URL: http://base.garant.ru/12148555/(Время обращения 12.12.2019г.)
4. Стратегия национальной безопасности РФ (Указ Президента РФ от 31 декабря 2015 г. N 683), URL: http://base.garant.ru/71296054/(Время обращения 12.12.2019г.)
5. Федеральный закон от 02.12.1990 N 395-1 (ред. от 02.12.2019) "О банках и банковской деятельности" URL:https://legalacts.ru/doc/FZ-o-bankah-i-bankovskoj-dejatelnosti/(Время обращения 12.12.2019г.)
6. Защита информации в вычислительных системах / Храмов В.В., Садовов В.В., Трубников А.Н., Губарев О.К.// Учебное пособие для вузов / Москва, 2002.-192с. URL: https://elibrary.ru/item.asp?id=32762286 (Время обращения 12.12.2019г.)
7. Модель специальной программной закладки / Храмов В.В., Трубников А.Н. Вопросы защиты информации. 1998. № 1-2 (40-41). С. 36-37. URL: https://elibrary.ru/item.asp?id=36309954 (Время обращения 12.12.2019г.)
8. Модель элементарной защиты программного средства / Храмов В.В., Трубников А.Н. // В сборнике: Информационные технологии и проблемы микроэлектроники. Сборник научных статей. под ред. докт. тех. наук, проф. В.А. Бархоткина. Москва, 1999. С. 192-197. URL: https://elibrary.ru/item.asp?id=327112590 (Время обращения 12.12.2019г.)
9. Основы методологии синтеза средств защиты информации / Храмов В.В. // В сборнике: Проблемы обеспечения эффективности и устойчивости функционирования сложных технических систем Материалы XXI Межведомственной научно-технической конференции. 2002. С. 115-120. URL: https://elibrary.ru/item.asp?id=32877301 (Время обращения 12.12.2019г.) (Время обращения 12.12.2019г.)
10. Информационная безопасность и защита информации на транспорте / Голубенко Е.В., Ковтун О.Г., Храмов В.В.// Тестовые задания по дисциплине / Ростов-на-Дону, 2015. URL: https://elibrary.ru/item.asp?id=36311930 (Время обращения 12.12.2019г.
11. Analysis of the aggressiveness of a software product / Khramov V.V., Trubnikov A.N.// Automatic Control and Computer Sciences. 1999. Т. 33. № 2. С. 28-34. URL: https://elibrary.ru/item.asp?id=13328155 (Время обращения 12.12.2019г.)
12. Способ повышения безопасности программных средств и пути его реализации / Губарев О.К., Храмов В.В. // В сборнике: Тематический научно-технический сборник Пущино, Научный Центр РАН, 1994. С. 56-61. URL: https://elibrary.ru/item.asp?id=32837963 (Время обращения 12.12.2019г.)

Ответы

1 Общая проблема информационной безопасности информационных систем

1.1 Информация как объект и предмет защиты

1.1.1 Важность; полнота; толерантность.

1.1.2 Важность; полнота; адекватность.

1.1.3 Конфиденциальность.

1.1.4 3, 1, 5, 6, 2, 4.

1.1.5 Контроля доступа к объектам; обеспечения конфиденциальности и целостности информации; апеллируемости действий.

1.1.6 Идентификации субъектов; обеспечения конфиденциальности и целостности информации; апеллируемости действий.

1.1.7 Идентификации субъектов; аутентификации и авторизации; контроля доступа к объектам.

1.1.8 Политика.

1.1.9 Атак.

1.1.10 Уязвимости.

1.1.11 Специалистов по безопасности, которые хотят проверить уровень уязвимости ИС своей организации; специалистов по сертификации информационных систем с точки зрения ИБ; организаций, предоставляющих услуги по анализу защищенности ИС; злоумышленников, использующих сканеры для поиска основы при реализации атаки.

1.1.12 Антивирусное.

1.1.13 Межсетевые.

1.1.14 Сканеры безопасности.

1.1.15 Информационная безопасность.

1.1.16 Безопасность.

1.1.17 Верификация.

1.1.18 Государственная тайна.

1.1.19 Защищенность.

1.1.20 Технология.

1.1.21 Информация.

1.1.22 Компонент.

1.1.23 Защита.

1.1.24 Закладка.

1.1.25 Программно-аппаратные закладки; загрузочные и драйверные закладки; прикладные и исполняемые закладки; закладки-имитаторы.

1.1.26 Надежность.

1.1.27 Отказоустойчивость.

1.1.28 Аутентификация.

1.1.29 Доступность.

1.1.30 Политика.

1.2 Угрозы, уязвимости и риски информационной безопасности

1.2.1 Угроза.

1.2.2 Создание отказоустойчивых КС, минимизация ущерба от стихийных бедствий; оптимизация взаимодействия человека с КС, блокирование ошибочных операций, дублирование информации, повышение надежности КС.

1.2.3 Шпионаж; диверсии; использование вредительских

программ и программных закладок; несанкционированный доступ.

1.2.4 Физическое проникновение злоумышленника к источнику информации; сотрудничество органа разведки или злоумышленника с работником конкурента; дистанционный съем информации с носителя.

1.2.5 Шпионаж; диверсия.

1.2.6 Утечка информации.

1.2.7 Случайными, непреднамеренными.

1.2.8 Угрозой.

1.2.9 Разработчик КС; сотрудник из числа обслуживающего персонала; пользователь; постороннее лицо.

1.2.10 Вычисления ускоряются и упрощаются; нет необходимости присваивать денежную стоимость активу; нет необходимости вычислять частоту проявления угрозы и точный размер ущерба; не нужно вычислять соответствие эффективности предполагаемых мер угрозам.

1.2.11 Риск.

1.2.12 Ущербом.

1.2.13 Отказы и сбои аппаратуры; Помехи на линии связи от воздействий внешней среды; ошибки человека как звена системы.

1.2.14 Системные и системотехнические ошибки разработчиков; структурные, алгоритмические и программные ошибки; аварийные ситуации.

1.2.15 Уязвимость.

1.2.16 Критичность.

1.2.17 Преднамеренные.

1.2.18 Раскрытие содержания передаваемых сообщений; анализ трафика, позволяющий определить принадлежность отправителя и получателя данных к одной из групп пользователей сети, связанных общей задачей; изменение потока сообщений, что может привести к нарушению режима работы какого-либо объекта, управляемого из удаленной ЭВМ.

1.2.19 Изменение потока сообщений, что может привести к нарушению режима работы какого-либо объекта, управляемого из удаленной ЭВМ; неправомерный отказ в предоставлении услуг; несанкционированное установление соединения.

1.3 Экономика информационной безопасности и инструменты оценки ее уровней

1.3.1 Защищенности.

1.3.2 Потенциального.

1.3.3 Четыре.

1.3.4 Осязаемым.

1.3.5 Неосязаемых.

1.3.6 Информационный.

1.3.7 Построения модели ИС с позиции ИБ; оценки ценности ресурсов; составления списка угроз и уязвимостей, оценки их характеристик; выбора контрмер и анализа их эффективности; анализа вариантов построения защиты; документирования (генерация отчетов).

1.3.8 Ресурс.

1.3.9 Критичность.

1.3.10 Критичное.

2 Защита информации при реализации информационных процессов

2.1 Организационное обеспечение информационной безопасности

2.1.1 1, 2, 3, 4, 5, 6.
2.1.2 Параллельными; сдублированными.
2.1.3 Эффективность.
2.1.4 Организационные.
2.1.5 Организационные.
2.1.6 Обработка и хранение конфиденциальных документов; контроль системы конфиденциального документооборота.
2.1.7 Блокирования.
2.1.8 Многоуровневая.
2.1.9 Организационные.
2.1.10 Полное или частичное перекрытие каналов утечки информации; объединение всех используемых средств защиты в целостный механизм.

2.2 Технологическое обеспечение информационной безопасности

2.2.1 Разграничение доступа; идентификация и аутентификация; аудит; управление политикой безопасности; криптографические функции.
2.2.2 Система разграничения доступа к информации.
2.2.3 Матричный; полномочный (мандатный).
2.2.4 Обязательное.
2.2.5 Избирательное; полномочное.
2.2.6 Чтение; выполнение программ; запись.
2.2.7 Полномочия.
2.2.8 Матрица.
2.2.9 Полномочный или мандатный метод.
2.2.10 Блок идентификации и аутентификации субъектов доступа; диспетчер доступа; блок криптографического преобразования информации при ее хранении и передаче.
2.2.11 Идентификации и аутентификации субъектов доступа; диспетчер доступа.
2.2.12 Ядро.
2.2.13 Недекларированные.
2.2.14 Маршрут.
2.2.15 Информационный.

2.3 Техническое обеспечение информационной безопасности

2.3.1 Технический канал утечки информации.
2.3.2 Радиомикрофоны, электронные «уши», устройства перехвата телефонных сообщений; устройства приема, записи, управления, видеосистемы наблюдения, записи и охраны.
2.3.3 Системе стандартизации и унификации; системе лицензирования деятельности; системе сертификации средств защиты; системе сертификации

технических средств и объектов информатизации; системе аттестации защищенных объектов информатизации.

2.3.4 Систему инженерно-технических и организационных мер охраны; систему регулирования доступа; систему режима и контроля вероятных каналов утечки информации; систему мер возврата материальных ценностей.

2.3.5 Многорубежность построения охраны по нарастающей; комплексное применение современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации; надежное инженерно-техническое перекрытие вероятных путей несанкционированного вторжения в охраняемые пределы.

2.3.6 Устойчивую систему связи и управления всех взаимодействующих в охране структуры; высокую подготовку и готовность основных и резервных сил охраны к оперативному противодействию преступным действиям; самоохрану персонала.

2.3.7 Объективное определение «надежности» лиц, допускаемых к работе; максимальное ограничение количества лиц, допускаемых на объекты предприятия; установление для каждого работника (или посетителя) дифференцированного по времени, месту и виду деятельности права доступа на объект; четкое определение порядка выдачи разрешений и оформления документов для входа (въезда) на объект.

2.3.8 Определение объемов контрольно-пропускных функций на каждом проходном пункте; оборудование контрольно-пропускных пунктов техническими средствами, обеспечивающими достоверный контроль и объективную регистрацию проходящих; высокую подготовленность и защищенность персонала контрольно-пропускных пунктов.

2.3.9 Реализация разрешительной системы допуска исполнителей к работам, документам и информации конфиденциального характера; разграничение доступа пользователей к данным АС различного уровня и назначения; учет документов, информационных массивов, регистрация действий пользователей ИС; снижение уровня и информативности ПЭМИН.

2.3.10 Снижение уровня акустических излучений; активное зашумление в различных диапазонах; противодействие оптическим и лазерным средствам наблюдения; проверка технических средств и объектов информатизации на предмет выявления включенных в них закладных устройств («жучков»).

2.4 Защита информации от несанкционированного доступа

2.4.1 Сбоях, отказах КС; наличии слабых мест в комплексной системе защиты информации.

2.4.2 Несанкционированный.

2.4.3 Правилами.

2.4.5 Закладка.

2.4.6 Закладки.

2.4.7 Терминалы пользователей; терминал администратора системы; терминал оператора функционального контроля; средства отображения информации.

2.4.8 Средства загрузки программного обеспечения; средства документирования информации; носители информации; внешние каналы связи.

2.4.9 Обоснованность доступа, когда исполнитель должен иметь соответствующую форму допуска для ознакомления с информацией определенного уровня конфиденциальности; персональную ответственность за сохранность доверенных пользователю информационных массивов, за свои действия в информационных системах; надежность хранения, когда информационные массивы хранятся в условиях, исключающих несанкционированное ознакомление с ними, их уничтожение, подделку или искажение.

2.4.10 Разграничение информации по уровню конфиденциальности, а также предупреждение передачи конфиденциальной информации по незащищенным линиям связи; контроль за действиями пользователей с документацией, а также в автоматизированных системах и системах связи; очистку оперативной памяти, буферов при освобождении пользователем до перераспределения этих ресурсов между другими пользователями; целостность технической и программной среды.

2.4.11 Контрольная сумма.

2.4.12 интернет-конфликт, связанный с проникновением в компьютерные системы и сети других стран.

2.4.13 Неприкосновенность информации.

2.4.14 Конфиденциальность, доступность, целостность.

2.4.15 Группа защитников окружающей среды запускает атаку типа «Отказ в обслуживании» против нефтяной компании, ответственной за крупную утечку нефти.

2.4.16 Выявление недостатков сетей и систем для повышения уровня безопасности этих систем.

2.4.17 Двухфакторная аутентификация, шифрование данных, идентификация по имени пользователя и паролю.

2.4.18 Получения привилегированного доступа к устройствам без раскрытия себя.

2.4.19 Переходит на новые компьютеры без какого-либо вмешательства и без ведома пользователя, является саморазмножающейся.

2.4.20 устранение способности целевой цели атаки обрабатывать другие запросы.

2.4.21 Перехват пакетов.

2.4.22 Nmap.

2.4.23 Увеличить веб-трафик на вредоносные сайты.

2.4.24 Антишпионское ПО.

2.4.25 Открывать веб-браузер в режиме конфиденциального просмотра.

2.4.26 Подключаться через VPN-сервис.

2.4.27 Шифрование данных.
2.4.28 ноутбук требует авторизации пользователя для обмена файлами и мультимедиа.
2.4.29 Облачный сервис.
2.4.30 Большинство устройств IoT не получают регулярные обновления микропрограммного ПО.
2.4.31 Предотвращение трансляции SSID.
2.4.32 Всегда отключать Bluetooth, когда он активно не используется.
2.4.33 mk$$cittykat104#.
2.4.34 Snort.
2.4.35 IDS.
2.4.36 DDoS.

3 Математические и методические средства защиты

3.1 Методы и модели обеспечения информационной безопасности

3.1.1 фильтрации.
3.1.2 Решетчатой модели безопасности.
3.1.3 1-й класс.
3.1.4 Пальца.
3.1.5 Запрет чтения информации субъектом с уровнем безопасности меньше чем у объекта чтения; запрет записи информации субъектом с уровнем безопасности больше чем объект, в который записывается информация.
3.1.6 Адепт 50.
3.1.7 Модель Гогена – Мезигера.
3.1.8 Водяных.
3.1.9 Нестандартная разметка (форматирование) носителя информации.
3.1.10 Субъекта/программы/объекта.
3.1.11 Блока контроля среды размещения программы.
3.1.12 Оптимальная.
3.1.13 Временная.
3.1.14 Временная.
3.1.15 Оптимальная.

3.2 Криптографические методы защиты информации

3.2.1 Тайнопись.
3.2.2 Алгоритм шифрования должен базироваться на небольшом объеме секретной информации.
3.2.3 Секретный ключ; закрытый ключ.
3.2.4 Размер ключа равняется или превышает размер исходного текста.
3.2.5 Таблице.
3.2.6 Повторном.
3.2.7 Поточное.
3.2.8 Побитно.
3.2.9 С одноразовым или бесконечным ключом; с конечным ключом; на основе генератора псевдослучайных чисел.
3.2.10 Бит шифрования, получающийся на каждом новом шаге автомата.
3.2.11 Блочное.

3.2.12 Поточном.
3.2.13 Периодом.
3.2.14 Симметричном.
3.2.15 Известному.
3.2.16 Вправо.
3.2.17 Циклический сдвиг влево.
3.2.18 Комбинирующий; фильтрующий; динамический.
3.2.19 Блочное.
3.2.20 Исключающее ИЛИ; НЕ.
3.2.21 Блочных.
3.2.22 DES.
3.2.23 Перестановка бит/расширение блока с помощью повторов по определенной схеме; наложение ключа раунда операцией XOR; табличные подстановки; перестановка бит.
3.2.24 Программы Diskreet; специализированной микросхемы.
3.2.25 Ориентированность на программную реализацию; слишком малый размер ключа.
3.2.26 56.
3.2.27 Файштеля.
3.2.28 ГОСТ 28147-89.
3.2.29 Советского Союза.
3.2.30 От таблицы подстановок.
3.2.31 Потенциальная емкость ключа в 256 бит; взятое с «запасом» число раундов.
3.2.32 ГОСТ 28147-89.
3.2.33 Блочных.
3.2.34 Время.
3.2.35 Отказах.
3.2.36 1991.
3.2.37 1993.
3.2.38 Асимметричное.
3.2.39 Единственный результативный метод атаки на него – полный перебор всех возможных ключей.
3.2.40 Открытый ключ; секретный ключ; закрытый ключ.
3.2.41 Асимметричное шифрование.
3.2.42 Асимметричном.
3.2.43 Открытым.
3.2.44 Асимметричное.
3.2.45 2N.
3.2.46 Схема RSA.
3.2.47 Евклида.
3.2.48 Рабина.
3.2.49 Квадрат.
3.2.50 Эль-Гамаль.
3.2.51 Ключей.
3.2.52 Полиномиальное.
3.2.53 Эллиптической.
3.2.54 Исправлением.
3.2.55 48.

3.3 Электронная цифровая подпись

3.3.1 Аутентичность отправителя; целостность сообщения.
3.3.2 Электронная цифровая подпись.
3.3.3 Рабина.
3.3.4 Логарифма.
3.3.5 Эль-Гамаля.
3.3.6 Схема Рабина; Схема Эль-Гамаля.
3.3.7 Эллиптических.
3.3.8 Алгоритм.
3.3.9 На вход алгоритма преобразования может поступать двоичный блок данных произвольной длины; на выходе алгоритма получается двоичный блок данных фиксированной длины; значения на выходе алгоритма распределяются по равномерному

закону по всему диапазону возможных результатов; при изменении хотя бы одного бита на входе алгоритма его выход значительно меняется: в идеальном случае инвертируется произвольная половина бит.

3.3.10 Зная результат хэш-функции, невозможно подобрать, кроме как полным перебором, какой-либо входной блок данных, дающий такое же значение на выходе; невозможно подобрать, кроме как полным перебором, пару различных входных блоков, дающих на выходе произвольный, но одинаковый результат.

3.3.11 128.

3.3.12 Как поступать с данными, не кратными числу (k – n); как добавлять в хэш-сумму длину документа, если это требуется; как разбивать исходный текст на блоки.

3.3.13 Хэш-функции.

3.3.14 Рабина.

3.3.15 Процессы.

3.4 Методология построения защищенных автоматизированных систем

3.4.1 Агрегирование; интерференция; комбинация разрешенных запросов для получения закрытых данных.

3.4.2 Блокировка ответа; искажение ответа; разделение БД; случайный выбор записи; контекстно-ориентированная защита; контроль поступающих запросов.

3.4.3 Фильтрации.

3.4.4 UNIX(r)-хосты; операционные системы Microsoft Windows NT&153; Windows(r) 95 и другие, поддерживающие стек протоколов TCP/IP; интеллектуальные принтеры, имеющие IP-адрес; X-терминалы.

3.4.5 1, 2, 3, 4.

3.4.6 Перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности; перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий; матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС; режим обработки данных в АС.

3.4.7 Разработчиком.

3.4.8 Наличие в АС информации различного уровня конфиденциальности; уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации; режим обработки данных в АС – коллективный или индивидуальный.

3.4.9 Три.

3.4.10 3Б; 3А.

3.4.11 2А; 2Б.

3.4.12 1Д; 1Г; 1В; 1Б; 1А.

3.4.13 Управления доступом; регистрации и учета; криптографической; обеспечения целостности.

3.4.14 Подлинности.

3.4.15 Идентификаторов.

4 Компьютерные средства реализации защиты в информационных системах

4.1 Программные закладки

4.1.1 Внесение произвольных искажений в коды программ, находящихся и оперативной памяти компьютера; искажения, выводящие на внешние компьютерные устройства или в канал связи информацию, полученную в результате работы других программ; организация «зависаний» компьютера.

4.1.2 Драйверные.

4.1.3 Выполнение операции записи в операционную или внешнюю память.

4.1.4 Выполнение операции записи в операционную или внешнюю память.

4.1.5 Программные.

4.1.6 Искажение, подмена результатов функционирования программы; нарушение функционирования программы; уничтожение информации; нелегитимный перехват, передача данных и сохранение фрагментов информации, обрабатываемых программой; модификация кода программы.

4.1.7 Способу доставки в систему; специфике расположения; отношению к программе-носителю; длительности скрытого периода; целевой эффективности.

4.1.8 Агрессивный.

4.1.9 Агрессивности.

4.1.10 Агрессивности.

4.2 Вредительские программы

4.2.1 Вирусы.

4.2.2 Качественные и визуальные; обнаруживаемые средствами тестирования и диагностики; качественные и визуальные; обнаруживаемые средствами тестирования и диагностики.

4.2.3 Логические.

4.2.4 Звуковые эффекты; уничтожение файлов и другие аналогичные действия.

4.2.5 Вирус.

4.2.6 В оперативную память ЭВМ; в каждую работающую программу.

4.2.7 Сканирование; эвристический анализ; аппаратно-программные антивирусные средства.

4.2.8 Запустить антивирусную программу; проверить на отсутствие загрузочных вирусов и файловых вирусов.

4.2.9 Открыть квадратное отверстие.

4.2.10 Нарушение адресации; сбой устройств; «зависание системы».

4.2.11 Выключить ЭВМ для уничтожения резидентных вирусов.

4.2.12 Червями.

4.2.13 Троянские кони.

4.2.14 Комплексная.

4.3 Протоколы безопасности

4.3.1 Аутентификация.
4.3.2 Туннелированием.
4.3.3 Узлом.
4.3.4 Разграничение доступа; идентификация и аутентификация; аудит; управление политикой безопасности; криптографические функции; сетевые функции.
4.3.5 1, 2, 3.
4.3.6 3.
4.3.7 Объектом.
4.3.8 Соответствует идентификатору запроса, на который посылается ответ.
4.3.9 Алгоритм.
4.3.10 Арбитр.

4.4 Защита от обратного проектирования

4.4.1 Программа «А», состоящая из исходных или объектных файлов; стандартные библиотеки, используемые программой; фрагмент кода, который извлекается из программы, будет подвержен трансформации.
4.4.2 Набор трансформирующих процессов; фрагмент кода, который извлекается из программы, будет подвержен трансформации; набор функций, которые будут определять важность фрагмента кода и задавать определенное значение переменной «RequireObfuscation».
4.4.3 Набор функций, которые будут определять важность фрагмента кода и задавать определенное значение переменной «RequireObfuscation»; числовая переменная «AcceptCost» > 0, которая хранит информацию о доступном максимальном увеличении системных ресурсов, потребующихся исходной программе; числовая переменная «RequireObfuscation» > 0, которая хранит значение требуемого уровня осуществления обфускации.
4.4.4 Код программы в результате трансформации будет существенно отличаться от кода исходной программы, но при этом он будет выполнять те же функции и оставаться работоспособным; при каждом процессе трансформации одного и того же кода исходной программы коды измененных программ будут различны.
4.4.5 Процесс реверсивной инженерии измененной программы будет более сложным, трудоемким и занимать больше времени, чем исходной программы; создание средства, детрансформирующего измененную программу в первоначальный вид, будет неэффективно.
4.4.6 Устойчивость.
4.4.7 Эластичность.
4.4.8 Стоимость.
4.4.9 1, 3, 2, 4.
4.4.10 2, 3, 1.
4.4.11 Удаление всех комментариев в коде программы или изменение их на дезинформирующие; удаление пробелов и отступов; замену идентификаторов на произвольные длинные наборы символов, которые трудно воспринимать человеку; добавление различных лишних операций;

изменение расположения блоков программы, так, чтобы это не повлияло на ее работоспособность.

4.4.12 Удаление всех комментариев в коде программы или изменение их на дезинформирующие; удаление пробелов и отступов; добавление различных лишних операций; изменение расположения блоков программы, так, чтобы это не повлияло на ее работоспособность.

4.4.13 Удаление всех комментариев в коде программы или изменение их на дезинформирующие; удаление пробелов и отступов; замену идентификаторов на произвольные длинные наборы символов, которые трудно воспринимать человеку; добавление различных лишних операций.

4.4.14 Обфускацию хранения; обфускацию соединения; обфускацию переупорядочивания.

4.4.15 Добавление различных лишних операций; разделение переменных фиксированного диапазона на две и более переменных.

4.4.16 Изменение интерпретации данных определенного типа; разделение переменных фиксированного диапазона на две и более переменных.

4.4.17 Изменение срока использования хранилищ данных – перехода от локального их использования к глобальному и наоборот; разделение переменных фиксированного диапазона на две и более переменных.

4.4.18 Объединение переменных; реструктурирование массивов; изменение иерархий наследования классов.

4.4.19 Объединение переменных; реструктурирование массивов; изменение иерархий наследования.

4.4.20 Объединение переменных; реструктурирование массивов; изменение иерархий наследования классов.

4.4.21 Обфускация вычислительная; обфускация соединения; обфускация последовательности.

4.4.22 Обфускация вычислительная; обфускация соединения; обфускация превентивная.

4.4.23 Обфускация соединения; обфускация последовательности; обфускация превентивная.

4.4.24 Превентивная.

4.4.25 Устойчивости; эластичности; стоимость преобразования.

5 Программа информационной безопасности России и пути ее реализации

5.1 Документы по информационной безопасности государства

5.1.1 Тайна.

5.1.2 Носители.

5.1.3 Защиты.

5.1.4 Допуск.

5.1.5 Доступ.

5.1.6 Реквизиты.

5.1.7 Перечень.

5.1.8 Обоснованность.

5.1.9 Сертификат.

5.1.10 Принятие на себя обязательств перед государством по нераспространению доверенных им

сведений, составляющих государственную тайну; письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий; ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение.

5.1.11 Документированная.

5.1.12 Государства.

5.1.13 Собственник.

5.1.14 Документированной.

5.1.15 Риск.

5.1.16 Потребителе.

5.1.17 Арбитражным.

5.1.18 Открытой.

5.1.19 Правонарушениях.

5.1.20 Третейские.

5.1.21 Национальные.

5.1.22 Информационной.

5.1.23 Реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности; совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство; противодействие угрозе развязывания противоборства в информационной сфере.

5.1.24 Национальных.

5.1.25 Повысить безопасность ИС; интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью; обеспечить защиту сведений, составляющих государственную тайну; расширять международное сотрудничество Российской Федерации в области противодействия угрозе противоборства в информационной сфере.

5.1.26 Монополизация информационного рынка России отечественными и зарубежными информационными структурами; блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории; низкая эффективность информационного обеспечения государственной политики РФ.

5.1.27 Деятельность иностранных политических, экономических, военных и информационных структур, направленная против интересов РФ в информационной сфере; стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве; обострение международной конкуренции за обладание информационными технологиями и ресурсами; увеличение технологического отрыва ведущих держав мира и их противодействие созданию конкурентоспособных российских информационных технологий.

5.1.28 Снижение степени защищенности законных интересов граждан, общества и государства в информационной сфере; недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере; недостаточное финансирование мероприятий по обеспечению ИБ РФ; снижение эффективности

системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения ИБ.

5.1.29 Создание системы противодействия монополизации информационных услуг и СМИ; активизация пропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

5.1.30 Информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики РФ; распространение за рубежом дезинформации о внешней политике РФ; нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом; попытки несанкционированного доступа к информации и воздействия на информационные ресурсы РФ.

5.2 Обеспечение практической безопасности

5.2.1 Непреднамеренные ошибки.

5.2.2 Угрозы раскрытия; угроза целостности; угроза отказа в обслуживании.

5.2.3 Атак.

5.2.4 Сканер.

5.2.5 наиболее простой метод обнаружения атак; позволяет жестко увязать образец с атакой; сообщение об атаке достоверно (если образец верно определен); применим для всех протоколов.

5.2.6 Если образец определен слишком обще, то вероятен высокий процент ложных срабатываний; если атака нестандартная, то она может быть пропущена; для одной атаки, возможно, придется создавать несколько образцов; метод ограничен анализом одного пакета и, как следствие, не улавливает тенденций и развития атаки.

5.2.7 В применении метод лишь ненамного сложнее метода сравнения с образцами; позволяет жестко увязать образец с атакой; сообщение об атаке достоверно (если образец верно определен); применим для всех протоколов; уклонение от атаки более сложно (по сравнению с методом сравнения с образцами).

5.2.8 Если образец определен в общем виде, то вероятен высокий процент ложных срабатываний; если атака нестандартная, то она может быть пропущена.

5.2.9 Снижает вероятность ложных срабатываний, если протокол точно определен; позволяет жестко увязать образец с атакой; позволяет улавливать различные варианты на основе одной атаки; позволяет обнаружить случаи нарушения правил работы с протоколами.

5.2.10 Если стандарт протокола допускает разночтения, то вероятен высокий процент ложных срабатываний; метод сложен для настройки.

5.2.11 Пакете.

5.2.12 Потоком.

5.2.13 Пакетный.
5.2.14 Контролем.
5.2.15 Приложения.
5.2.16 Возможность влияния на функционирование МСЭ со стороны пользователя ЭВМ; более высокая стоимость владения: помимо закупочной цены необходимо учитывать стоимость распределенной поддержки.
5.2.17 Третьего.
5.2.18 Второго.
5.2.19 Первого.
5.2.20 Межсетевой.
5.2.21 Текст сообщения должен быть доступен только отправителю и адресату; неотрекаемость; апеллируемость; возможность отправить письмо, оставшись анонимным.
5.2.22 Установить программу фильтр для E-mail.
5.2.23 Карт.
5.2.24 Неполнота и неопределенность исходной информации о составе ИС и характерных угрозах; многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей СЗИ; наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения СЗИ; невозможность применения классических методов оптимизации.
5.2.25 1, 2, 3, 4, 5, 6, 7.
5.2.26 Реализации правил фильтрации; процесса регистрации; процесса идентификации и аутентификации администратора МСЭ; процесса контроля за целостностью программной и информационной части МСЭ; процедуры восстановления.
5.2.27 Агентов.
5.2.28 Межсетевой.
5.2.29 Экранирование.
.

6 Нормативно-правовые аспекты информационной безопасности.

6.1 Международные стандарты защиты информации

6.1.1 «Оранжевая книга»; TCSEC.
6.1.2 ITSEC.
6.1.3 CTCPEC.
6.1.4 A1; B3; B2; B1.
6.1.5 B3.
6.1.6 Аутентификации партнеров; конфиденциальности; целостности соединения.
6.1.7 Аутентификации партнеров; целостности соединения; безотказности.
6.1.8 Конфиденциальности; секретности трафика; безотказности.
6.1.9 Безотказности.
6.1.10 Конфиденциальности.
6.1.11 «Оранжевая книга».
6.1.12 «Красная книга».
6.1.13 Стандарт CCITSE.
6.1.14 Аутентификацию, управление доступом, конфиденциальность данных, целостность данных, безотказность.
6.1.15 C2 «Оранжевой книги».
6.1.16 Автоматическую реакцию в случае потенциального нарушения

безопасности; генерирование данных аудита; хранение событий аудита.

6.1.17 Среду безопасности; требования информационной безопасности.

6.1.18 Автоматическое управление конфигурацией; область действия.

6.1.19 Функциональную спецификацию; соответствие представлений; моделирование политики безопасности.

6.1.20 Анализ скрытых каналов; злоупотребление.

6.1.21 Определение атрибутов пользователя; спецификация секретов; привязка пользователя к субъекту.

6.1.22 Истечение атрибутов безопасности.

6.1.23 Анонимность; разрыв связи; неотслеживаемость.

6.1.24 Ограничение на объем атрибутов; блокирование сессий; история доступа к объекту оценки.

6.1.25 Сбой безопасности; обнаружение повтора; разделение доменов.

6.1.26 Стандарт CCITSE.

6.1.27 Защита носителей информации.

6.1.28 Кадровая безопасность.

6.1.29 Оценка рисков.

6.1.30 Мониторинг регуляторов безопасности.

6.2 Правовое регулирование отношений, связанных с информационными технологиями

6.2.1 Аккредитации.

6.2.2 Профиль.

6.2.3 Правовым.

6.2.4 Обслуживания силами специальных организаций; создания собственной службы безопасности.

6.2.5 Стандартизация; лицензирование.

6.2.6 Федеральная служба безопасности РФ; Федеральная служба охраны РФ; Федеральная служба по техническому и экспортному контролю; Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

6.2.7 Лицензии.

6.2.8 Неправомерного доступа к охраняемой законом компьютерной информации.

6.2.9 Несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети; создание, использование и распространение вредоносных компьютерных программ.

6.2.10 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

6.2.11 Штраф до 200 тысяч рублей или лишение свободы до 2 лет.

6.2.12 Штраф от 100 до 300 тысяч рублей или лишение свободы на срок до 4 лет.

6.2.13 Лишение свободы на срок до 4 лет со штрафом до 200 тысяч рублей.

6.2.14 Лишение свободы на срок до 5 лет со штрафом от 100 до 200 тысяч рублей.

6.2.15 Лишение свободы на срок до 7 лет.

6.2.16 Штраф до 500 тысяч рублей или лишение свободы до 2 лет.
6.2.17 По законодательству страны проживания пользователя; по законодательству страны проживания собственника ресурса; по законодательству страны проживания владельца.

6.3 Государственная система обеспечения информационной безопасности РФ

6.3.1 Безопасности.
6.3.2 Норм.
6.3.3 «О безопасности».
6.3.4 Гражданском кодексе Российской Федерации.
6.3.5 Уголовном кодексе Российской Федерации.
6.3.6 Вредоносных.
6.3.7 «Об участии в международном информационном обмене».
6.3.8 «Об информации, информатизации и защите информации».
6.3.9 Персональные данные.
6.3.10 Служебную тайну.
6.3.11 Коммерческую тайну.
6.3.12 «О техническом регулировнии».

Краткий словарь терминов

Авторизация – проверка полномочий или проверка права пользователя на доступ к конкретным ресурсам и выполнение определенных операций над ними.

Аутентификация – установление подлинности пользователя, представившего идентификатор, или проверка того, что лицо или устройство, сообщившее идентификатор, является действительно тем, за кого оно себя выдает. Наиболее распространенным способом аутентификации является присвоение пользователю пароля и хранение его в компьютере.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (закон РФ от 21 июня 1993 г. № 5485-1 «О государственной тайне»).

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него (закон РФ от 21 июня 1993 г. № 5485-1 «О государственной тайне»).

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений (закон РФ от 21 июня 1993 г. № 5485-1 «О государственной тайне»).

Доступ к информации – возможность получения информации и ее использования (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Доступ к информации, составляющей коммерческую тайну – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации (федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне»).

Доступ к сведениям, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление

конкретного лица со сведениями, составляющими государственную тайну (закон РФ от 21 июня 1993 г. № 5485-1 «О государственной тайне»).

Идентификация – присвоение пользователю (объекту или субъекту ресурсов) уникальных имен и кодов (идентификаторов).

Информация – сведения (сообщения, данные) независимо от формы их представления (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Информация, составляющая коммерческую тайну, – научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны (федеральный закон от 29 июля 2004 г. N 98-ФЗ).

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Информационная безопасность АСОИ – состояние рассматриваемой автоматизированной системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить

доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду (федеральный закон от 29 июля 2004 г. N 98-ФЗ).

Контрагент – сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию (федеральный закон от 29 июля 2004 г. N 98-ФЗ).

Несанкционированный доступ – доступ к информации, который нарушает правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов (закон РФ от 21 июня 1993 г. № 5485-1 «О государственной тайне»).

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Объект доступа – единица информации автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Криптостойкость – характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.

Обладатель информации, составляющей коммерческую тайну, – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении нее режим коммерческой тайны (федеральный закон от 29 июля 2004 г. N 98-ФЗ).

Правила разграничения доступа – совокупность правил, регламентирующих права субъектов доступа к объектам доступа.

Передача информации, составляющей коммерческую тайну, – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности (федеральный закон от 29 июля 2004 г. N 98-ФЗ).

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Предоставление информации, составляющей коммерческую тайну, – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций (федеральный закон от 29 июля 2004 г. N 98-ФЗ).

Разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору (федеральный закон от 29 июля 2004 г. N 98-ФЗ).

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Режим коммерческой тайны – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности (федеральный закон от 29 июля 2004 г. N 98-ФЗ).

Санкционированный доступ – доступ к информации, который не нарушает правил разграничения доступа.

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях (закон РФ от 21 июня 1993 г. № 5485-1 «О государственной тайне»).

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации (закон РФ от 21 июня 1993 г. № 5485-1 «О государственной тайне»).

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Электронный документ – документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах (федеральный закон от 27 июля 2006 г. № 149-ФЗ).

Учебное издание

Алекперов Ильгар Джаби оглы
Храмов Владимир Викторович
Горбачева Анастасия Александровна
Фомичев Дмитрий Павлович

ТЕСТОВЫЕ ЗАДАНИЯ ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В ЦИФРОВОЙ ЭКОНОМИКЕ»

Подписано в печать 30.12.19. Формат 60×84/16.
Бумага газетная. Ризография. Усл. печ. л. 6,04.
Тираж 100 экз. Изд. № 104. Заказ

Редакционно-издательский центр ЮУ (ИУБиП).

Адрес университета:
344038, Ростов-на-Дону, пр. М. Нагибина 33А/47