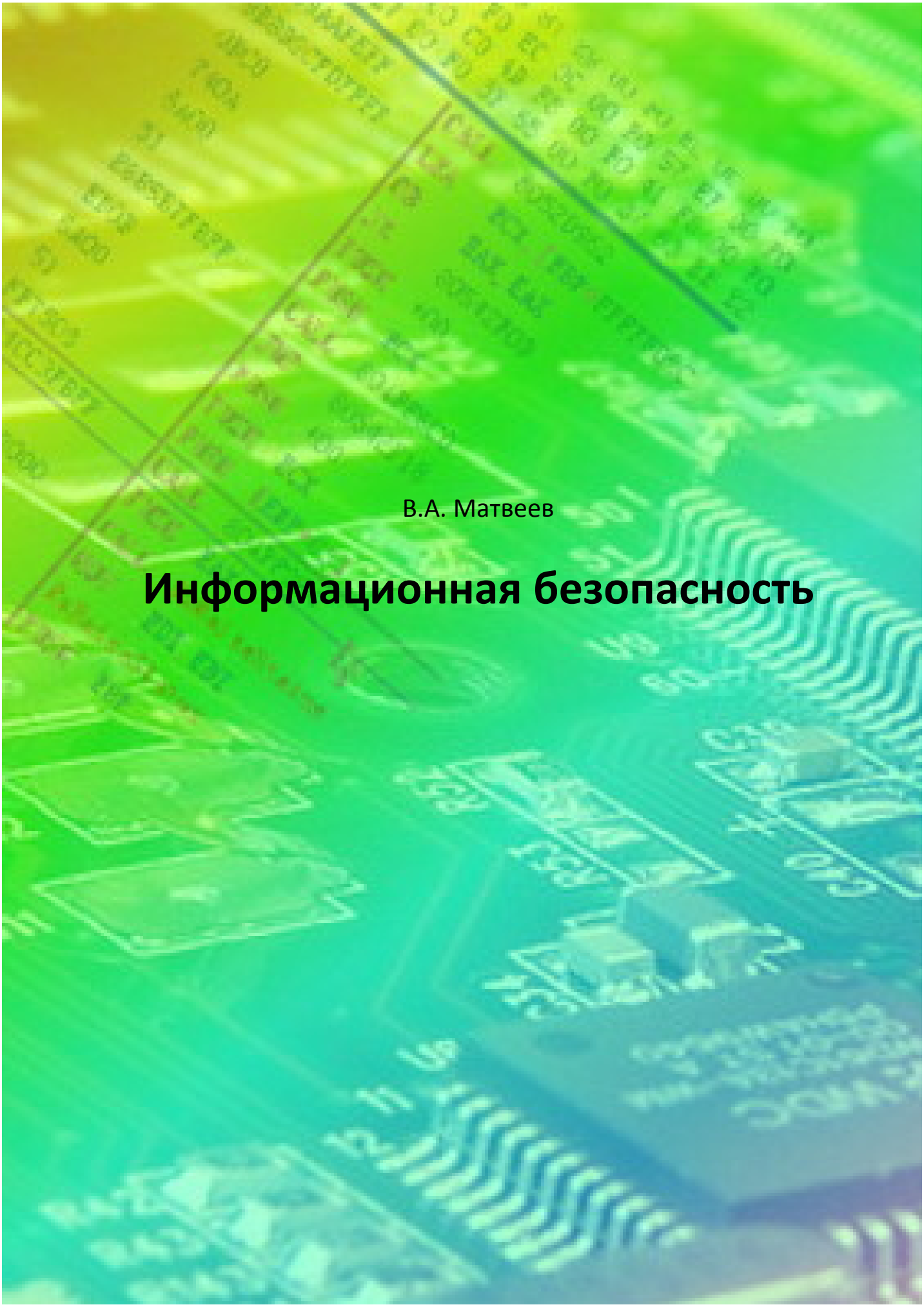

В.А. Матвеев

Информационная безопасность

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ НИЖЕГОРОДСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Н.И. ЛОБАЧЕВСКОГО»

ИНСТИТУТ ЭКОНОМИКИ И ПРЕДПРИНИМАТЕЛЬСТВА

Матвеев В.А.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебно-методическое пособие

Нижний Новгород, 2017 г.

УДК 311(075.8)

ББК У051

М 33

М-33 Матвеев В.А. Информационная безопасность: Учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2017.

Учебно-методическое пособие отражает краткое содержание основных разделов, методические указания для проведения практических занятий и контрольные вопросы для организации текущего контроля по учебной дисциплине «Информационная безопасность».

УДК 311(075.8)

ББК У051

Содержание

Тема 1. Теоретические основы информационной безопасности

Методические указания

Развитие человеческого общества неразрывно связано с процессом информатизации, под которым понимается непрерывно возобновляемый процесс создания необходимых условий для удовлетворения информационных потребностей человека. На протяжении всей истории человеческой цивилизации и даже на начальной стадии возникали потребности, связанные с получением, хранением и накоплением, первичной обработкой и переработкой, поиском, отображением, передачей и обменом информацией.

Современный этап информатизации характеризуется созданием информационных систем и систем телекоммуникации с применением средств персональной электронной вычислительной техники.

В результате накопления мирового практического опыта, знаний и духовных ценностей границы национальных экономик постепенно стираются и формируется информационное общество, которое развивается в соответствующем информационном пространстве.

Под инфосферой понимается сфера практической деятельности по сбору, созданию, получению, хранению, преобразованию, распространению и использованию информации, неразрывно связанная с информационной инфраструктурой и соответствующими субъектами, а также системами регулирования возникающих при этом общественных отношений.

Информационная сфера выполняет системообразующую функцию жизни информационного общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности государства, личности и общества. Таким образом, национальная безопасность существенным образом зависит от обеспечения информационной безопасности.

По мере развития человеческой цивилизации, интеграции национальных экономик, глобализации информационных процессов накапливаются противоречия, которыми неизбежно определяется любое развитие, в виде реальных военных конфликтов, противостояния национальных, личных интересов, которые постепенно переходят и в информационную сферу.

Под информационной безопасностью понимается состояние защищенности от информационных угроз, сохранение свойств объекта информационной безопасности, которые обусловлены информацией, её потоками и информационной инфраструктурой.

В соответствии с Указом Президента от 9 мая 2017 г. №203 утверждена Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы. Для обеспечения информационной безопасности на законодательном уровне разрабатывается механизм, позволяющий согласовать процесс разработки законов и подзаконных нормативных актов и развития современных информационных технологий. Он включает совокупность мер, направленных на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности путем принятия соответствующих законодательных актов, а также направляющие и координирующие меры (государственный контроль за информационными процессами, система государственной статистической отчетности, разработка и внедрение национальных сертифицированных средств защиты информации, систем электронных платежей, денег и торговли, стандартизация этих систем и разработка нормативной правовой базы, регламентирующей их использование, совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики и т.д.).

Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 5.12.2016 г., представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения национальной безопасности РФ в информационной сфере.

Для изучения нормативно-правовых основ обеспечения информационной безопасности запустим информационную систему Консультант Плюс и создадим папку с фамилией в разделе «Избранное» с помощью соответствующей кнопки.

В разделе «Карточка поиска» заполнить следующие поля следующими данными: «Вид документа» – «Федеральный закон»; «Дата» - «01.06.2006 – 31.08.2006» с помощью кнопки «Диапазон дат»; «Название документа» – «О защите информации».

Построить список документов с помощью кнопки «Показать список документов», выбрать документ с именем №149-ФЗ «Об информации…» в последней редакции и открыть его. В тексте документа произвести поиск понятия «Конфиденциальность информации», для чего с помощью кнопки «Найти» заполнить соответствующее поле. Вызвать контекстное меню элемента слева он найденного понятия, выбрать пункт «Добавить в избранное», вкладку «Закладки и документы и нажать кнопку «Добавить». Проверить в разделе «Избранное наличие соответствующей закладки.

Сохранить найденный документ в папку «Фамилия» с помощью последовательности пунктов «Добавить в избранное» – «Папки» – «Фамилия» и проверить наличие документа в папке «Фамилия». Аналогично найти Доктрину информационной безопасности РФ и Федеральный закон «О персональных данных» №152-ФЗ, сохранить их в папку «Фамилия» и поставить закладки для понятий «Персональные данные», «Уничтожение персональных данных» и «Правовые методы обеспечения информационной безопасности». Аналогично найти Федеральные законы «Об электронной подписи» и «О коммерческой тайне", сохранить их в папку «Фамилия» и поставить закладки для нескольких понятий.

С помощью кнопки «Словарь терминов» заполнить поле «Найти» следующими данными «Электронная цифровая подпись» или «ЭЦП», перейти по ссылке найденного документа и добавить это понятие в закладки, присвоив имя закладке «ЭЦП». Аналогично поставить закладки понятий «Электронное правительство» и «Информационная безопасность организации банковской системы РФ».

В разделе «Кодексы» перейти по ссылке «Уголовный кодекс РФ» и произвести поиск статей, касающихся компьютерных преступлений с помощью кнопок «Найти» и «Найти далее», а также экспортировать найденную статью (глава 28) в Microsoft Word с помощью соответствующей кнопки. Аналогично произвести поиск статей, касающихся налоговой тайны, а также экспортировать найденную статью в Microsoft Word.

В разделе «Карточка поиска» в поле «вид документа» ввести «Статья» и построить список документов из трех статей, касающихся обеспечения информационной безопасности, и экспортировать в Microsoft Word.

Контрольные вопросы по теме

1. Понятие информатизации
2. Этапы развития информационных технологий
3. Признаки информационного общества
4. Понятие информационного пространства
5. Понятие информационной войны и информационной преступности
6. Понятие информационной безопасности
7. Субъекты и объекты информационной безопасности
8. Нормативно-правовые основы информационной безопасности
9. Понятие экономической информации
10. Перечень сведений конфиденциального характера

Контрольные задания 1

Используя информационную систему Консультант Плюс, найти и отобразить с добавлением в раздел «Избранное» и экспортом в Microsoft Word:

1) основные нормативно-правовые акты, регулирующие деятельность в информационной сфере;

2) определения основных категорий информационной безопасности;

3) подборку статей по защите информации.

Тема 2. Принципы построения системы защиты информации

Методические указания

Защита информации – это научно организованный систематический процесс планирования и реализации наиболее рациональных и эффективных в современных условиях мероприятий, применения всего комплекса методов и средств, которые гарантируют определенный уровень информационной безопасности, обеспечивают контроль состояния системы защиты информации, своевременное выявление ее уязвимых мест и противоправных действий в отношении объекта защиты.

Под системой защиты информации понимается система органов, средств, методов, технических, технологических, административных и иных мер и конкретных мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз, безопасность функционирования информационной системы, ее аппаратных и программных средств, связанных с ними информационных ресурсов, коммуникаций и т.д.

Существует два принципиальных подхода к обеспечению информационной безопасности: комплексный и фрагментарный. Они базируются на нескольких принципах, носящих общий или специфический характер. К числу общих можно отнести принципы единства, конечной цели, иерархии, связности, модульного построения, развития, функциональности, децентрализации и неопределенности.

Реализации функций системы защиты информации обеспечивается подсистемам правового, организационного, аппаратного, информационного, программного, математического, лингвистического, нормативно-методического и иного обеспечения.

Рассмотрим реализацию функций системы защиты информации на примере стандартных средств, доступных пользователям операционной системы Windows.

Учетная запись – это набор данных, который характеризует возможности пользователя по доступу к ресурсам операционной системы, настройке общих, групповых и индивидуальных параметров работы (например, политика сетевой безопасности, темы оформления, фоновые рисунки, общие и индивидуальные папки, файлы, ярлыки и т.д.).

Каждый пользователь операционной системы получает доступ к собственной или групповой учетной записи с помощью логина и пароля, который указывается при создании учетной записи. Индивидуальность логина и степень сложности пароля повышают уровень защищенности от несанкционированного доступа (длина пароля не менее 8 символов, комбинированное использование буквенно-цифрового кода, регистров и т.д.).

При этом необходимо указать один из типов доступа:

- административные – полный контроль на ресурсами операционной системы и ее настройками;
- ограниченные – отсутствие доступа к определенным настройкам операционной системы, запуску и установке определенного программного обеспечения и т.д.

После создания учетной записи возможно осуществление операций изменения и удаления.

Создать учетную запись можно используя пункты главного меню операционной системы «Пуск», «Панель управления», «Создание учетной записи». Аналогичную операцию можно произвести с помощью контекстного меню «Мой компьютер», «Управление компьютером», подраздела «Локальные пользователи». В нем имеется две категории:

- пользователи, которыми могут быть собственно пользователи операционной системы
- группы, которыми могут быть администраторы, операторы архива, гости и т.д.

Используя пункты меню «Действие», «Новый пользователь» и «Свойства» можно выбрать необходимый тип учетной записи:

- администраторы, которые имеют доступ ко всем ресурсам операционной системы и ее настройкам;
- пользователи – могут выполнять большинство пользовательских функций (запуск программ, использование сетевого и локального принтера, завершение работы операционной системы и т.д.), а также могут создавать локальные группы,

регулировать их состав, однако не могут получить доступ к общим папкам, создавать локальные принтеры и т.д.;

- операторы архива, которые могут осуществлять архивирование и восстановление файлов в операционной системы, а также вход в операционную систему и завершение ее работы, однако не имеют прав изменения настроек безопасности;
- гости – могут выполнять регистрацию пользователей с помощью учетной записи «Гость» и получать ограниченные права на доступ к ресурсам и настройкам операционной системы;
- опытные пользователи, которые могут создавать учетные записи пользователей, модифицировать настройки безопасности только для создаваемых ими учетных записей, создавать локальные группы и модифицировать состав ее участников, а также аналогичные операции с группами «Пользователи», «Гости» и «Опытные пользователи», однако не могут модифицировать участие в группах «Администраторы» и «Операторы архива», не могут быть владельцами файлов, производить архивирование и восстановление фалов, загружать и выгружать драйверы устройств и модифицировать настройки безопасности и журнал событий;
- репликаторы – участником группы могут быть только учетные записи, с помощью которых можно зарегистрироваться в службе репликации контроллера домена, при этом они не должны создавать рабочие учетные записи.

Контрольные вопросы по теме

1. Понятие и функции системы защиты информации
2. Общие принципы обеспечения информационной безопасности
3. Специальные принципы обеспечения информационной безопасности
4. Обеспечивающие подсистемы защиты информации

Контрольные задания 2

Используя справочные средства операционной системы Windows найти и отобразить с экспортом в Microsoft Word:

1) понятия учетной записи и домена и типов доступа к операционной системе: глобальные, локальные, ограниченные и административные;
2) описание порядка создания, изменения, активации и удаления учетных записей;
3) основные категории локальных пользователей (пользователи и группы) и конкретных прав каждого вида учетных записей, включая администраторов, пользователей, опытных пользователей, операторов архива, репликаторов и гостей.

Тема 3. Классификация угроз информационной безопасности

Методические указания

Под угрозой информационной безопасности понимается случайное или преднамеренное явление или событие, действие или процесс, которые могут привести к искажению, несанкционированному использованию или к уничтожению информационных ресурсов информационной системы, используемых программных и технических средств и соответственно прямому или косвенному моральному или материальному ущербу интересам общества, личности или государства (например, ущерб деловой репутации, необходимость восстановления нарушенных защищаемых информационных ресурсов, невозможность выполнения взятых на себя обязательств перед третьей стороной, снижение эффективности политики государства и т.д.). Реализация угроз информационной безопасности заключается в частичном или полном нарушении работоспособности информационной системы, а также утрате ценности или частичном обесценивании информации в случае нарушения: а) конфиденциальности (при хранении и распространении информации); б) целостности (при изменении или уничтожении информации); в) доступности информации (в случае неполучения или несвоевременного получения информации легальным пользователем).

Информационные угрозы по способу реализации можно разделить на три группы: разглашение, утечка и несанкционированный доступ. В последнем случае имеет место противоправное преднамеренное ознакомление с конфиденциальной информацией недопущенных лиц, нарушение целостности (подделка, модификация, уничтожение) и доступа к защищаемой информации. Информационные угрозы по отношению к объекту информационной безопасности можно подразделить на две основные группы: внутренние и внешние; по причине возникновения на две основные группы: естественные (например, стихийные бедствия, аварии электропитания) и человеческие, которые подразделяются по характеру возникновения на две основные группы: случайные и преднамеренные.

В последнем случае имеет место целенаправленное воздействие на аппаратные, программные и информационные ресурсы, несанкционированное использование информационных ресурсов по личным противоправным мотивам (например, с целью нанесения ущерба пользователям информационной системы), не оказывая при этом влияния на состояние информационной системы (пассивные) или нарушая нормальный процесс функционирования информационной системы (активные).

Вредоносное программное обеспечение можно подразделяется на такие классы, как файловые и загрузочные вирусы, компьютерные черви, «троянский конь», макровирусы, логические бомбы, стелс-вирусы (невидимки), полиморфные вирусы (вирусы-призраки) и «бэкдоры».

Компьютерная преступность – это умышленное нарушение чужих прав и интересов, осуществляемое совершаемые с помощью компьютеров, информационных систем и телекоммуникаций или направленные против них, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства с определенными целями.

В наиболее общем виде компьютерных преступлений можно классифицировать по способу совершения на следующие основные группы: несанкционированный доступ, вирусная модификация (разработка, использование или распространение компьютерных вирусных программ, которые заведомо приводят к нарушению работы ЭВМ или их сетей, внесению несанкционированных собственником изменений в компьютерную информацию) и перехват информации.

Рассмотрим практические способы защиты от вредоносных программ. Для поиска и обезвреживания (лечения, удаления) вредоносных программ, блокирующих работу операционной системы, осуществляющих удаление, модификацию, шифрование данных, несанкционированный доступ к конфиденциальный информации и ее передачу (например, троянские программы) существует разнообразное антивирусное программное обеспечение. Для операционной системы Windows могут применяться антивирусные программы Kaspersky Antivirus, Doctor Web, NOD, McAfee и т.д., которые, как правило, могут

функционировать в автономном (offline) и сетевом режиме (online), что объясняется необходимостью обновления антивирусных баз, нештатным режимом функционирования операционной системы (блокирование доступа пользователя к ресурсам операционной системы, всплывающие окна, ошибки в работе, отказ устройств и т.д.). В наиболее сложных ситуациях при затрудненном пуске операционной системы может потребоваться загрузка антивирусной программы в безопасном режиме, которая позволяет осуществить очистку реестра и ресурсов операционной системы от следов вредоносного кода.

Помимо проверяемой области (оперативная память, локальный диск, съемный накопитель), типов проверяемых файлов и порядка действий при обнаружении вредоносной программы, как правило, можно выбрать уровень безопасности работы (высокий, рекомендуемый или низкий) в зависимости от уровня квалификации пользователя, а также метод проверки: эвристический анализ – позволяет обнаружить новые модификации кода вредоносного программного обеспечения, которые отсутствуют в базе антивирусной программы с различными уровнями детализации в зависимости от степени тщательности проверки; поиск сигнатур – облегчает нахождение известных угроз безопасности и устранение уязвимостей в установленном программном обеспечении и параметрах операционной системы на основании кодовых записей (сигнатур), содержащихся в базе антивирусной программы; поиск руткитов – обнаружение вредоносных программ, которые скрывают свою активность в операционной системе.

Запустим антивирусную программу McAfee – сканирование по требованию и настроим параметры ее работы. Во вкладке «Объекты сканирования» указать проверяемую область (все локальные диски), отметить пункты, касающиеся вложенных папок и загрузочных секторов, в разделе «Элементы» – отметить пункты, касающиеся запущенных процессов и руткитов, а также добавить элемент «Зарагистрированные файлы» с помощью кнопки «Добавить». Во вкладке «Сканировать элементы» выбрать типы проверяемых файлов по умолчанию и дополнительные типы (.zip), отметить пункт, касающийся макросов, в разделе «Параметры» – отметить пункт, касающийся архивов, а в разделе «Эвристический анализ» – отметить все пункты. Во вкладке «Производительность» перевести элемент «Использование системы» в состояние «Ниже нормы». Во вкладке «Действия» выбрать в качестве порядка: первое действие – «Вывести запрос», второе действие – «Удалить». Во вкладке «Отчеты» с помощью кнопки «Обзор» создать файл отчета «Фамилия» на рабочем столе. В главном меню антивирусной программы запустить проверку и контролировать результаты работы.

Контрольные вопросы по теме

1. Понятие информационной угрозы
2. Причины реализации информационных угроз
3. Виды реализации угроз информационной безопасности
4. Классификация информационных угроз
5. Способы воздействия информационных угроз
6. Классификация вредоносного программного обеспечения
7. Классификация компьютерных преступлений

Контрольные задания 3

Используя средства Internet (kaspersky.ru и т.п.), справочные средства и антивирусное программное обеспечение:

1) найти и отобразить с экспортом в Microsoft Word понятия мошеннического программного обеспечения, харкерских атак, фишинга и спама;
2) найти и отобразить с экспортом в Microsoft Word описание порядка использования и ключевых функций Kaspersky Unlocker и Kaspersky Internet Security, дать сравнительную характеристику ключевых функций Kaspersky Rescue Disk и Kaspersky Antivirus (Kaspersky Virusscanner, Kaspersky Virus Removal Tool и т.д.).
3) открыть антивирусную программу, произвести настройку параметров ее работы, запустить проверку и сформировать отчет от результатах работы.

Тема 4. Методы и средства обеспечения информационной безопасности

Методические указания

К методам обеспечения информационной безопасности принято относить препятствие; управление доступом, включая идентификацию и аутентификацию объекта или субъекта, проверку полномочий, регистрацию обращений и реагирование; маскировку, регламентацию, принуждение и побуждение.

Эти методы реализуются с помощью следующих основных средств: законодательные, организационные, аппаратные, программные, криптографические и т.д.

В частности, организационные средства обеспечения информационной безопасности - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий. Оно включает в себя ряд административных, технических и экономических мероприятий.

Криптографический механизм включает следующие основные элементы: шифрование данных, которое может быть симметричным (основывается на использовании одного и того же секретного ключа для шифрования и дешифрования) и асимметричным (для шифрования используется один общедоступный ключ, а для дешифрования - другой, являющийся секретным, при этом знание общедоступного ключа не позволяет определить секретный ключ); цифровая электронная подпись (основываются на алгоритмах ассиметричного шифрования и включают две процедуры: формирование подписи отправителем путем шифрования блока данных с использованием секретного ключа и ее опознавание получателе, основанная на использовании общедоступного ключа); контроль доступа (осуществляют проверку полномочий программ и пользователей на доступ к ресурсам информационной сети.); управление маршрутизацией обеспечение целостности данных (обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем: отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку) и аутентификации и так далее.

Продемонстрируем на практике применение криптографических методов обеспечения информационной безопасности. Как известно, коды использовали в глубокой древности для засекречивания какого-либо важного сообщения Геродот, Цезарь, Бэкон и другие. Сегодня при передаче сообщений по линиям связи используются те или иные коды, т.е. представление сообщения в виде комбинации элементарных сигналов или символов (например, азбука Морзе).

Кодированием называется отображение состояния одной физической системы с помощью состояния некоторой другой (например, при телефонном разговоре звуковые сигналы кодируются в виде электромагнитных колебаний, а затем снова декодируются, превращаясь в звуковые сигналы на другом конце линии).

Криптология (от греч. kryptos – тайный, logos – наука) разделяется на два направления – криптографию и криптоанализ. Криптография (от греч. grafos – письмо) – наука о защите информации от несанкционированного доступа. Сфера интересов криптоанализа противоположная – разработка и исследование методов дешифрования (раскрытия) шифрограммы даже без знания секретного ключа.

Под шифрованием понимается такое преобразование информации, которое делает исходные данные нечитаемыми и трудно раскрываемыми без знания ключа, т.е. специальной секретной информации, определяющей, какое преобразование из множества возможных шифрующих преобразований выполняется в конкретном случае над открытым текстом.

По характеру использования ключа алгоритмы шифрования делятся на два типа: симметричные (с одним секретным ключом) и несимметричные (с открытым и закрытым ключами или с одним открытым ключом).

Множество современных методов шифрования можно разделить на четыре большие группы: метод подстановки – позиции символов в шифрованном сообщении остаются теми

же, что и у исходного открытого сообщения, однако символы заменяются символами из другого или этого же алфавита (например, в квадрате Полибия буквы заменяются соответствующими цифрами); метод перестановок – все символы исходного открытого сообщения остаются без изменений, но меняются местами по определенному закону с использованием определенного ключа; аддитивные методы – порядковые номера (коды) символов исходного сообщения увеличиваются (уменьшаются) на величину каждого из символов (кодов) последовательности, которая называется гаммой шифра; аналитическое преобразование – производится преобразование структурных блоков исходного сообщения в соответствии с определенным алгоритмом; комбинированные методы – сочетание вышеназванных методов.

Метод перестановки может реализовываться с помощью матричного алгоритма, который заключается в том, что исходные символы текста помещаются в матрицу слева направо и сверху вниз, а затем производится шифрование путем считывания символов по столбцам матрицы сверху вниз слева направо, при этом количество столбцов и порядок их считывания является ключом шифра; вместо ключа возможно использование ключевого слова, в котором число букв и их алфавитное расположение определяет алгоритм перестановки).

ИЯАЦРМФОИН – ИНФОРМАЦИЯ
РКПИОТРГФАЯИ – КРИПТОГРАФИЯ

О	Т	О	Б	Р	А
Ж	Е	Н	И	Е	И
Н	Ф	О	Р	М	А
Ц	И	И			

ВАРИАНТ КОДА А:
Ключ: 6 столбцов
ОЖНЦТЕФИОНОИБИРРЕМАИА

ВАРИАНТ КОДА Б:
Ключевое слово: данные
ТЕФИОЖНЦАИАОНОИБИРРЕМ

При использовании метода подстановки в простейшем случае для дешифрации ключ может быть известен или находится путем визуального анализа шифрованного сообщения (например, порядковые номера букв в алфавите), а при неизвестном ключе применяется методы статистического анализа.

10 15 22 16 18 14 1 24 10 33 – ИНФОРМАЦИЯ

Повторяемость ключевого слова при наличии достаточно большого объема у шифра накладывает некоторый отпечаток на криптограмму, а это может быть обнаружено статистическими методами, которые позволяют судить о длине ключевого слова, после чего расшифровка значительно упрощается.

Для этого в шифрованном сообщении определяется абсолютные и относительные показатели повторяемости отдельных символов (частоты и частости). Затем производится их ранжирование, для чего необходимо упорядочить относительные частоты повторяемости по убыванию. После этого необходимо установить тесноту и характера корреляционной связи между рядом распределения исходного сообщения и типичным рядом распределения относительных частот повторяемости букв русского алфавита.

Буква	Частость	Буква	Частость
пробел, знак препинания	0,175	П	0,023
А	0,062	Р	0,040
Б	0,014	С	0,045
В	0,038	Т	0,053
Г	0,013	У	0,021
Д	0,025	Ф	0,002
Е	0,084	Х	0,009
Ё	0,001	Ц	0,004
Ж	0,009	Ч	0,012

З	0,016	Ш	0,006
И	0,062	Щ	0,003
Й	0,012	Ъ	0,004
К	0,028	Ы	0,018
Л	0,035	Ь	0,016
М	0,026	Э	0,003
Н	0,053	Ю	0,006
О	0,090	Я	0,018

При этом необходимо учитывать как синтаксический аспект исходного сообщения, начиная с расшифровку с наиболее вероятных совпадений тесно коррелирующих символов (пробел, буквы О, Е, А и т.д.) и разбивая исходный текст на структурные блоки, так и семантический аспект сообщения, устанавливая отношение отдельных элементов шифра к общей системе.

Например, расшифруем следующий код методом подстановки без ключа:

10 32 25 30 11 16 12 26 11 4 12 26
10 22 24 10 14 4 18 20 30 25 30 26
10 13 15 6 13 8 32 10 14 20 24 26
13 26 8 32 16 29 18 16 21 26 11 30
4 8 16 30 26 28 21 14 31 26 23 16
30 25 30 26 23 13 8 32 10 14 20 24
26 26 32 10 4 18 26 8 18 1 16 31
26 18 1 4 18 7 16 32 26 11 32 4
30 20 24 12 26 19 13 16 33 34 18 12
26 10 4 24 28 32 32 14 26 15 30 4
30 20 24 12 26 26 33 26 6 30 11 18
16 32 26 4 2 28 30 20 31 26 13 26
16 24 10 26 20 26 18 1 28 21 14 33
32 26 14 32 15 4 18 14 10 12 26 13
26 33 24 8 11 30 25 30 26 20 26 25
6 13 11 18 26 4 13 22 7 32 26 23
21 26 15 6 30 15 31 32 23 26 32 32
26 11 30 26 16 18 14 33 18 26 16 30
26 20 6 24 25 13 26 20 26 30 28 18
11 13 26 16 32 26 11 24 11 18 23 26
26 11 32 16 31 26 33 30 14 30 6 21
27 26 15 4 30 3 30 26 16 24 22 24
14 26 16 32 26 28 6 24 16 18 26 14

30 10 33 4 18 20 30 26 16 30 12 26
15 30 14 30 23 13 26 22 14 30 26 18
26 13 11 24 22 24 26 13 14 6 30 23
26 10 15 18 14 26 30 14 26 15 32 6
32 15 30 12 26 26 23 16 32 26 8 24
4 31 26 16 32 28 30 10 20 30 11 26
5 14 30 14 26 10 18 16 18 27 26 8
24 4 31 26 1 32 23 4 2 26 18 26
8 18 1 16 18 26 30 10 33 30 4 33
18 26 23 16 32 26 10 14 6 24 7 16
30 26 22 14 30 26 10 21 14 21 32 26
10 20 18 16 31 18 26 10 14 6 24 7
16 32 27 26 22 32 23 26 25 30 4 30
11 16 21 32 26 20 30 4 33 18 26 26
30 25 6 30 23 32 16 26 11 30 4 25
26 16 24 7 26 6 24 1 16 21 23 26
4 2 11 12 23 26 24 26 28 4 18 1
33 18 23 26 28 30 4 32 32 26 11 6
13 25 18 3 26 11 30 4 8 16 21 26
23 21 26 14 32 23 26 33 30 25 30 26
23 21 26 4 2 28 18 23 26 13 8 32
26 1 24 26 14 30 26 22 14 30 26 4
2 28 18 23 26 18 3

Первый шаг дешифровки – составление таблицы частот, частостей и рангов для кодов зашифрованного сообщения:

N	O	P	R
Счетчик	Частота	Частость	Ранг
1	=СЧЕТЕСЛИ ($A$1:$L$47;N1)=8	=O2/$O$36=0,015	=РАНГ(C1;$C$1:$C$34) =22
2	5	0,009124	25
3	3	0,005474	27
4	26	0,047445	6
5	1	0,001825	29
6	14	0,025547	13
7	5	0,009124	25
8	11	0,020073	18
9	0	0	33
10	19	0,034672	10
11	19	0,034672	10
12	9	0,016423	21
13	16	0,029197	12
14	26	0,047445	6
15	10	0,018248	20
16	31	0,056569	5

17	0	0	33
18	34	0,062044	3
19	1	0,001825	29
20	14	0,025547	13
21	12	0,021898	15
22	8	0,014599	22
23	20	0,036496	9
24	23	0,041971	8
25	11	0,020073	18
26	101	0,184307	1
27	3	0,005474	27
28	12	0,021898	15
29	1	0,001825	29
30	50	0,091241	2
31	8	0,014599	22
32	34	0,062044	3
33	12	0,021898	15
34	1	0,001825	29
Итого:	=СУММ(O1:O35)=548	=СУММ(P1:P35)=1	

Второй шаг дешифровки – установление соответствия кодов буквам русского алфавита.

Шифр	Дешифровка	Шифр	Дешифровка
26	пробел, знак препинания	8	Ы
30	О	25	Ь
18	Е	15	Г
32	А	12	З
16	И	1	Б
4	Н	22	Ч
14	Т	31	Й
24	С	2	Х
23	Р	7	Ж
10	В	3	Ш
11	Л	27	Ю
13	К	5	Ц
6	М	19	Щ
20	Д	29	Э
21	П	34	Ф
28	У	9	Ъ
33	Я	17	Ё

Третий шаг дешифровки – количественный анализ структуры шифрованного сообщения, выдвижение гипотезы относительно отклонения корреляции кодов шифрованного сообщения и букв русского алфавита в соответствии с языковыми особенностями (например, чередование гласных и согласных букв) и корректировка установленной корреляции.

С Е 25 30 Д Н 12 26 11 4 12 26
С 22 24 С Т 4 18 В О 25 О 26
10 13 15 6 13 8 32 10 14 20 24 26
13 26 8 32 16 29 18 16 21 26 11 30
4 8 16 30 26 28 21 14 31 26 23 16
30 25 30 26 23 13 8 32 10 14 20 24
26 26 32 10 4 18 26 8 18 1 16 31
26 18 1 4 18 7 16 32 26 11 32 4
30 20 24 12 26 19 13 16 33 34 18 12
26 10 4 24 28 32 32 14 26 15 30 4
30 20 24 12 26 26 33 26 6 30 11 18
16 32 26 4 2 28 30 20 31 26 13 26
16 24 10 26 20 26 18 1 28 21 14 33
32 26 14 32 15 4 18 14 10 12 26 13

26 33 24 8 11 30 25 30 26 20 26 25
6 13 11 18 26 4 13 22 7 32 26 В
Ы 26 15 6 30 15 31 32 23 26 Е Е
26 11 30 26 16 18 14 33 18 26 Н О
26 20 6 24 25 13 26 Я 26 30 28 18
11 13 26 Н А 26 11 24 11 18 23 26
26 11 32 16 31 26 33 30 14 30 6 21
27 26 15 4 30 3 30 26 16 24 22 24
14 26 16 32 26 28 6 24 16 18 26 14
30 10 33 4 18 20 30 26 16 30 12 26
15 30 14 30 23 13 26 Ч Т О 26 И
26 13 11 24 22 24 26 13 14 6 30 23
26 10 15 18 14 26 30 14 26 15 32 6
32 15 30 12 26 26 23 16 32 26 8 24

4 31 26 16 32 28 30 10 20 30 11 26
5 14 30 14 26 10 18 16 18 27 26 8
24 4 31 26 1 32 23 4 2 26 18 26
8 18 1 16 18 26 30 10 33 30 4 33
18 26 23 16 32 26 10 14 6 24 7 16
30 26 22 14 30 26 10 21 14 21 32 26
10 20 18 16 31 18 26 10 14 6 24 7
16 32 27 26 22 32 23 26 25 30 4 30
11 16 21 32 26 20 30 4 33 18 26 26

30 25 6 30 23 32 16 26 11 30 4 25
26 16 24 7 26 6 24 1 16 21 23 26
4 2 11 12 23 26 24 26 28 4 18 1
33 18 23 26 28 30 4 32 32 26 11 6
13 25 18 3 26 11 30 4 8 16 21 26
23 21 26 14 32 23 26 33 30 25 30 26
23 21 26 4 2 28 18 23 26 13 8 32
26 1 24 26 14 30 26 22 14 30 26 4
2 28 18 23 26 18 3

Четвертый шаг дешифровки – переход от отдельных элементов (букв, слов) к их системе, устанавливая общий смысл сообщения

С Е Г О Д Н Я Д Л Я
С Ч А С Т Л И В О Г О
10 13 15 6 13 8 32 10 14 20 24 26
13 26 8 32 16 29 18 16 21 26 11 30
4 8 16 30 26 28 21 14 31 26 23 16
30 25 30 26 23 13 8 32 10 14 20 24
26 26 32 10 4 18 26 8 18 1 16 31
26 18 1 4 18 7 16 32 26 11 32 4
30 20 24 12 26 19 13 16 33 34 18 12
26 10 4 24 28 32 32 14 26 15 30 4
30 20 24 12 26 26 33 26 6 30 11 18
16 32 26 4 2 28 30 20 31 26 13 26
16 24 10 26 20 26 18 1 28 21 14 33
32 26 14 32 15 4 18 14 10 12 26 13
26 33 24 8 11 30 25 30 26 20 26 25
6 13 11 18 26 4 13 22 7 32 26 В
Ы 26 15 6 30 15 31 32 23 26 Е Е
26 11 30 26 16 18 14 33 18 26 Н О
26 20 6 24 25 13 26 Я 26 30 28 18
11 13 26 16 32 26 11 24 11 18 23 26
26 11 32 16 31 26 33 30 14 30 6 21
27 26 15 4 30 3 30 26 16 24 22 24
14 26 16 32 26 28 6 24 16 18 26 14

30 10 33 4 18 20 30 26 16 30 12 26
15 30 14 30 23 13 26 Ч Т О 26 И
26 13 11 24 22 24 26 13 14 6 30 23
26 10 15 18 14 26 30 14 26 15 32 6
32 15 30 12 26 26 23 16 32 26 8 24
4 31 26 16 32 28 30 10 20 30 11 26
5 14 30 14 26 10 18 16 18 27 26 8
24 4 31 26 1 32 23 4 2 26 18 26
8 18 1 16 18 26 30 10 33 30 4 33
18 26 23 16 32 26 10 14 6 24 7 16
30 26 22 14 30 26 10 21 14 21 32 26
10 20 18 16 31 18 26 10 14 6 24 7
16 32 27 26 22 32 23 26 25 30 4 30
11 16 21 32 26 20 30 4 33 18 26 26
30 25 6 30 23 32 16 26 11 30 4 25
26 16 24 7 26 6 24 1 16 21 23 26
4 2 11 12 23 26 24 26 28 4 18 1
33 18 23 26 28 30 4 32 32 26 11 6
13 25 18 3 26 11 30 4 8 16 21 26
23 21 26 14 32 23 26 33 30 25 30 26
23 21 26 4 2 28 18 23 26 13 8 32
26 1 24 26 14 30 26 22 14 30 26 4
2 28 18 23 26 18 3

Контрольные вопросы по теме

1. Методы обеспечения информационной безопасности
2. Средства обеспечения информационной безопасности
3. Криптографическое обеспечение информационной безопасности
4. Организационное обеспечение информационной безопасности

Контрольные задания 4

1. Зашифровать следующие сообщения методом перестановки:

ИНФОРМАЦИОННЫЕ СИСТЕМЫ
ТЕЛЕКОММУНИКАЦИИ.

Зашифровать следующие сообщения методом подстановки:

КОНФИДЕНЦИАЛЬНОСТЬ
ШИФРОВАНИЕ
КРИПТОГРАФИЯ

Расшифровать следующее сообщение методом перестановки без ключа:

ЕЫНЬЛАНОСРЕП НАДЕЫН

2. Расшифровать следующий код методом перестановки, при известном ключе - РАДИАТОР:

сеиве неави ежвро еуррк _о_см т_тма же__с щемтр рмдры смввя ибяье аяаев
асммй о_о__ _а__ь нВо__ в_рд_ мра_ы повяя _дВжи уВсив _н_ее опмря яьнья
те

рврчр р_трк ряяья аяаеи яьясе аееeу вреае тмтмв мшром тмьуи вьрья ьписВ
иваВз исВав еб_р а__ л _м___ т_тмт ___я
ровяе р__ок емро_ тятмт _ымер н_ьят _еврс маквб амаен оимае аясар имятм
ятйс_ __ааи ят_би утбВт _лрбь ис_ри вляяе ипВзт __ьВн _ксъ_ ьяьрв нмаио
__ьо
рает_ тмт_т мтя__ ВеибВ зисет мьсья ьрьяь мья_б ___а_ _и_ее евоеи виВкр
яяаеа яаеас врмгр смррв _итрр _ррд_ ш
рчрое тмиее яяьят _инт_ _иеае рмьяд м__мт мия__ еяимм иг_юв н_ору Влввр
иеврн мо_оВ браВй е___ь л_еьв вр
тыю_а нсыи_ _ежЕд с_уак евавп амгчр Ч,ето _б__н с,био ,но_щ тд_ял _ечте
щеомд мосдм д_рео _т_от ст,_е ллеа_ нты_а ло_,м доте, бол_о еоаз, папЧз
атнот б_ьид у_и_: стама таьто __и_о р_у_о вдм__ з_р_р обуое ут_пь _тыяп
цт_ее __е

3. Расшифровать код методом подстановки при известном ключе:

24 33 44 34 36 32 11 46 24 63

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	ъ	ы	ь
6	Э	Ю	Я			

Расшифровать код методом подстановки при известном ключе:

7 8 2 25 23 10 15 23 28 1 5 20
18 2
7 25 4 33 23 14 8 18 5 20 33 18
10 14 24
8 25 5 32 14 5 11 28 8 14 15 5
28 5 15 14 11 24 5 8 2 28 19 18
30 5 11 33 19 33 23 5 4 2 14 8
5 6 18 22 33 20 5 20 33 18 20
32 14 5 8 14 6 25 1 5 10 14 11
14 5 3 28 20 18 2 25
32 14 5 4 2 33 18 7 32 33 10 18
5 18 20 14 32 18 5 19 33 10 4 33
8 25 5 11 33 19 25 5 15 23 33 14
19 33 5 32 25 4 2 25 10 32 33
29 14 10 15 21 5 8 32 14 1 5 2
25 11 33 15 25 1 5 5 18 5 8 14
6 25 1 5 23 10 24 3 18 14 5 8
14 6 25 5 10 23 33 18 5 25 5 8
14 32 21 5 10 14 8 21 20 17 1 5
19 33 10 4 33 8 28 5 11 33 19 28
5 15 23 33 14 20 28
4 33 34 18 15 25 1 5 33 15 22 25
5 15 23 33 14 19 33 5 18 5 20 25
15 21 5 15 23 33 16
32 14 5 28 11 18 23 25 1
32 14 5 4 2 14 6 16 11 33 8 14
1 10 15 23 28 1
32 14 5 3 2 25 8 18
32 14 5 4 2 33 18 7 32 33 10 18

5 6 33 13 32 33 19 33 5 10 23 18 8
14 15 14 6 21 10 15 23 25 5 32 25
5 11 6 18 13 32 14 19 33 5 15 23
33 14 19 33
32 14 5 13 14 6 25 1 5 8 33 20
25 5 11 6 18 13 32 14 19 33 5 15
23 33 14 19 33 5 32 14 5 13 14 6
25 1 5 13 14 32 17 5 11 6 18 13
32 14 19 33 5 15 23 33 14 19 33 5
32 18 5 2 25 11 25 5 14 19 33 5
32 18 5 33 10 6 25 5 14 19 33 5
32 18 34 14 19 33 5 34 15 33 5 28
5 11 6 18 13 32 14 19 33 5 15 23
33 14 19 33
7 25 4 33 23 14 8 18 5 20 33 30
25 20 20 14 8 25
32 14 5 4 2 18 8 25 23 25 1 5
19 33 10 4 33 8 28 5 10 33 15 33
23 25 2 18 27 14 1
32 14 5 28 11 18 23 25 1 5 8 14
15 14 1 5 10 23 33 18 30 5 2 25
8 18 5 11 14 8 32 33 10 15 18 5
10 23 33 14 1
2 33 8 18 15 14 6 24 20 5 11 6
25 19 33 8 14 24 32 18 14
10 33 15 23 33 2 24 1 5 20 33 6
18 15 23 28
11 33 1 10 24 5 20 14 2 7 33 10
15 14 1

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
25	11	23	19	8	14	9	13	7	18	1	3	6	20	32	33	4
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
2	10	15	28	12	30	22	34	29	27	31	17	21	26	16	24	5

Тема 5. Организация системы защиты информации

Методические указания

Построение системы защиты информации — это процесс поиска компромисса между уровнем защищенности и информационной системы и сохранением возможности ее работоспособности.

При построении системы защиты информации необходимо учитывать организационную структуру экономического объекта (организации, отрасли и т.д.); объем и характер информационных потоков, объем и характер выполняемых экономических операций и т.п.

Этапы построения системы защиты информации: анализ, оценка возможных и реальных информационных угроз, планирование, разработка проекта, реализация и постоянный контроль за качеством работой системы защиты информации.

К настоящему времени сформировались два основных способа реализации механизмов защиты: «добавленная» и «встроенная». В первом из них механизмы защиты не реализованы в программном и аппаратном обеспечении информационной системы или реализована только часть их, необходимая для обеспечения работоспособности всей информационной системы, а во втором – механизмы защиты являются неотъемлемой частью информационной системы, разработанной и реализованной с учетом определенных требований безопасности.

Обычно план содержит следующие группы сведений: политика безопасности, текущее состояние информационной системы, рекомендации по реализации системы защиты и ответственность персонала, порядок ввода в действие средств защиты и пересмотра плана и состава средств защиты.

Политика информационной безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и связанных с ней информационных ресурсов, и может быть избирательной и полномочной.

Избирательная политика информационной безопасности подразумевает, что все субъекты и объекты информационной системы должны быть идентифицированы; права доступа субъекта к объекту системы определяются на основании внешнего (по отношению к системе) правила. Полномочная политика информационной безопасности предполагает, что все субъекты и объекты системы однозначно идентифицированы; каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации; каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ. Основным ее назначением является регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновении с нижних уровней на верхние.

Основные функции служб информационной безопасности на этапе проектирования или совершенствования системы информационной безопасности заключаются в формировании требований к системе информационной безопасности и участие в разработке компонентов и системы информационной безопасности в целом, а на этапе эксплуатации – в планировании, организации и обеспечении функционирования системы информационной безопасности, обучении пользователей и технического персонала организации формам и методам эксплуатации технических средств и контроле за соблюдением пользователями и техническим персоналом правил работы и эксплуатации технических средств в части обеспечения информационной безопасности.

Резервное копирование (backup) – это процесс создания копии данных на носителей, предназначенных для их восстановления в случае повреждения или разрушения. Оно может быть полным, дифференциальным, когда хранятся изменения только по отношению к

последнему полному резервному копированию и инкрементным, когда хранятся изменения по отношению к последнему резервному копированию. Оно обеспечивает безопасность работы операционной системы, оперативное возобновления ее работоспособности, сохранность данных пользователей и т.д.

Обычно создается образ данных, включая все текущие настрои операционной системы, файлы пользователей, драйверов, программное обеспечение и т.д. Эта операция осуществляется при помощи специализированных программ (например, Norton Ghost, Acronis True Image, Partition Minitool и т.д.). После выбора источника «Source Drive» (например, системного раздела жесткого диска) можно присвоить имя образу, выбрать степень сжатия и активировать процесс записи образа, а затем и произвести восстановления данных из образа на локальном диске или его разделе (например, пункты главного меню «Local», «Disk» или «Partition», «To Image» или «To Partition», «From Image» или «From Partition») или на съемных накопителях.

В последнем случае для восстановления данных необходимо установить порядок загрузки операционной системы в соответствующих разделах BIOS («BIOS Features» или «Boot options», «Hard Disk Boot Priority», «First Boot Device», «Second Boot Device» и т.д.) меню которое можно вызвать до запуска операционной системы. Возможные состояния элементов, отвечающих за порядок загрузки: CDROM, Hard Disk, USB Flash и т.д. Дополнительную защиту от несанкционированного доступа позволяет получить раздел «Set supervisor password», который позволяет установить пароль на запуск операционной системы. После завершения этих операций необходимо сохранить внесенные изменения в параметры загрузки с помощью соответствующего раздела меню BIOS.

Контрольные вопросы по теме

1. Особенности и этапы построения системы защиты информации
2. Методы реализации механизмов защиты информации
3. План построения системы защиты информации
4. Функции службы информационной безопасности

Контрольные задания 5

Используя средства Internet и справочные средства программ резервного копирования найти и отобразить с экспортом в Microsoft Word:

1) понятия полного, дифференциального и инкрементного резервного копирования;

2) описание порядка создания образа и восстановления из него;

3) дать сравнительную характеристику основных функций трех программ резервного копирования по следующим критериям: условия распространения, планирование (работа по расписанию), возможности работы с разделами диска, создания загрузочного диска, шифрования, сжатия, настройки фильтров, онлайн резервного копирования.

Тема 6. Информационная безопасность отдельных экономических систем

Методические указания

Основные угрозы безопасности в современных информационных системах банков - вывод из строя, отказ в обслуживании, компрометация или подмена данных (утечка обрабатываемой конфиденциальной информации, ее искажение или разрушение в результате умышленного нарушения работоспособности информационной системы банка).

Безопасность информационной системы банка достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов системы.

К числу методов увеличения безопасности информационной системы банка относится применение системы регистрации и учета, непрерывная проверка на предмет возможного выявления специальных закладных устройств финансового шпионажа с целью получения несущих уязвимую информацию сигналов и т.д.

Существует несколько видов угроз электронной коммерции: проникновение в систему извне: несанкционированный доступ внутри компании и из одной сети в другую, преднамеренный перехват и чтение информации, преднамеренное нарушение данных или сетей, неправильная идентификация пользователя (с целями мошенничества), взлом программно-аппаратной защиты, вирусные атаки, отказ в обслуживании, финансовое мошенничество и т.д.

Для противодействия этим угрозам используется целый ряд методов: шифрование, электронные цифровые подписи, проверяющие подлинность личности отправителя и получателя; stealth-технологии с использованием электронных ключей; брандмауэры; виртуальные и частные сети.

Применение современных информационных технологии в бухгалтерском учете связано с такими угрозами информационной безопасности, как проникновение посторонних лиц в базы учетных данных, распространение компьютерных вирусов, фальсификация учетных данных, умышленный или непреднамеренный ошибочный ввод учетных данных (неверные коды, пропущенные учетные записи, несанкционированные учетные операции, ошибки при обработке или выводе данных, формировании или корректировке справочников, неполные учетные записи, неверное отнесение записей по периодам) и т.д.

Основный принцип, нарушаемый при реализации информационной угрозы в бухгалтерском учете, - это принцип документирования информации. Особую опасность представляют сведения, составляющие коммерческую тайну и относящиеся к учетной и отчетной информации (данные о партнерах, клиентах, банках и т.д.), поэтому необходимо оформить договора с сотрудниками бухгалтерии, финансовых служб и других экономических подразделений с указанием перечня сведений, не подлежащих огласке. Также существует угроза отрицания авторства отправителем с целью снятия с себя ответственности за передачу документа.

Для защиты от угроз информационной безопасности в практике обмена финансовыми документами (платежными поручениями, контрактами, распоряжениями) по компьютерным сетям используются методы аутентификации сообщений при отсутствии у сторон доверия друг к другу. Документ (сообщение) дополняется цифровой подписью и секретным криптографическим ключом. Подделка подписей без знания ключа посторонними лицами исключается и неопровержимо свидетельствует об авторстве.

Существует несколько уровней обеспечения информационной безопасности в среде «1С:Предприятие» для конфигурации «Бухгалтерский и налоговый учет». После запуска программы имеется два режима работы с системой: «1С: Предприятие», в котором проблема информационной безопасности решается на уровне пользовательского интерфейса и «Конфигуратор» - на уровне администратора.

В первом случае в разделе «Сервис» главного меню выберем пункт «Переключить интерфейс» и выберем один из списка интерфейсов с различным набором возможных операций (полный, административный, бухгалтерский, УСН, НДФЛ предпринимателя и т.д.).

Во втором случае сначала в системе введем несколько физических лиц – пользователей. Для этого в разделе «Кадры» главного меню выберем пункт «Физические лица» и заполним данными трех человек произвольно в окне «Личные данные физического лица» (например, «Имя» – «Иванов ИИ», «Код» – «00000001», «Дата рождения» – «01.01.01», «Пол» – «Мужской» и т.д.).

В разделе «Предприятие» главного меню выберем пункт «Организации» и произвольно введем данные своей фирмы (например, «МММ»).

В разделе «Предприятие» главного меню выберем пункт «Подразделения организаций» и произвольно введем данные (наименование и код) двух подразделений своей фирмы в окне «Список подразделений организации» (например, «администрация» – «00000002», «бухгалтерия» – «00000001»).

В разделе «Операции» главного меню выберем пункты «Справочники» и «Должности организаций» и произвольно введем данные (наименование и код) трех должностей в окне «Должности организации» (например, «администратор» – «00000002», «главный бухгалтер» – «00000001», «кассир» – «00000003»).

В разделе «Кадры» главного меню выберем пункт «Прием на работу» и на основе справочника «Физических лиц» (дата, код, организация и номер) введем данные трех сотрудников нашей фирмы в окне «Прием на работу. Проведен» от текущей даты (например, «Сотрудник» – «Иванов ИИ», «Номер» – «22000000001», «табельный номер» – «00000001», «Должность» – «Главный бухгалтер», «Вид расчета» - «Оклад по дням», «Размер» - «40000», «Подразделение» – «Бухгалтерия», «Дата приема» - «01.01.2017»

Затем установим пользовательский интерфейс и права доступа для каждого из сотрудников на уровне конфигуратора. Каждому пользователю можно установить роль и интерфейс из списка возможных, а также пароль доступа.

Для этого откроем «1С: Предприятие» в режиме «Конфигуратор». В разделе «Бухгалтерия предприятия» главного меню выберем пункты «Общие» и «Роли» или «Интерфейсы».

Роль – это набор прав по каждому объекту системы. Например, для роли «бухгалтер» по объекту «авансовый отчет» в окне «Роль бухгалтер: Права», можно отметить пункты по которым будут доступны соответствующие права (например, чтение, добавление, изменение, удаление и т.д.).

Интерфейсы – это набор объектов, которые доступны конкретному пользователю. Настроим, например, список панелей интерфейса «Бухгалтерский», а также разделы (подразделы) главного меню используя пункты «Главное меню, «Поддержка» (возможность обновлять конфигурации при их модификациях) и «Стандартные отчеты»

Для создания новых ролей и новых интерфейсов отключим конфигурацию от автоматического обновления используя раздел «Поддержка» и пункты «Настройка поддержки» и «Снять с поддержки».

Для реализации системы защиты создадим новую роль с именем «кассир» используя раздел «Роли» и пункт «Добавить».

Для конфигурации в целом поставим галочку «Толстый клиент», что обеспечит пользователю с ролью кассир право доступа в режиме «Толстого клиента», в котором работает конфигурация «Бухгалтерия».

Отметим все пункты для документа Приходный кассовый ордер и Расходный кассовый ордер.в окне «Роль кассир: Права», во вкладке «Права», поля «Объекты» и «Права».

Убедимся, что для остальных объектов не установлено никаких прав пользователя с ролью «кассир».

Создать новый интерфейс с именем «инткассир» в разделе «Конфигуратор», пункты «Интерфейсы», пункт контекстного меню «Добавить». В окне «Интерфейс: Инткассир: Интерфейс» удалим все разделы главного меню в поле «список панелей интерфейса» кроме «Файл» и «Операции» с помощью пункта контекстного меню «Удалить».

Затем с помощью пункта меню «Новая» введем в окне «Свойство: Элемент панели» в поле «Текст» - «Документ», «Тип кнопки» – «Подменю». После создания раздела главного меню «Документ» с помощью пункта «Новая» в окне «Выбор действия» выберем пункты соответствующие двум документам «ПКО» и «РКО» и убедимся в наличии в разделе «Документ» пунктов «РКО» и «ПКО».

Создадим связь роли «кассир» и интерфейса «инткассир» через пользователя «Иванов», для которого дополнительно установим пароль.

В разделе «Администрирование» выберем пункт «Пользователи» и введем пользователя с именем «Петров» с полными правами и интерфейсом «бухгалтерский» без паролей в окне «Пользователь», вкладки «Основные» и «Прочие», отметим пункт «Полные права» и поле «Основной интерфейс» переведем в состояние «Бухгалтерский».

Введем второго пользователя с именем «Иванов» с правами «кассир» и интерфейсом «инткассир» и введем любой пароль в поле «Пароль», а затем в поле «Подтверждение пароля».

Убеждаемся, что при входе в систему появляется возможность выбора пользователя, причем при входе для пользователя «Иванов» система потребует ввести пароль, а после входа отображается созданный интерфейс.

Дополнительно в окне «Роль кассир: Права» возможно усиление защиты на уровне реквизитов документа. Так, открыв перечень реквизитов ПКО, выберем, например, реквизит «счеткасса», для которого возможно установить и отменить права «просмотр» и «редактирование».

Кроме того, в режиме «Конфигуратор», выберем ветвь «Документы», раскроем реквизиты «ПКО», пункт «Данные». Раскроем пункт данные и в окне «Документ ПКО» выберем тот реквизит, который необходимо защитить, например, «валютаДокумента». Перейдем в ветвь «Формы», выберем пункт «Форма документа», поле «Валюта», вызовем окно «Свойства: Поле ввода» через контекстное меню. Убедимся, что в нем существует возможность изменения состояния каждого поля с помощью пунктов «видимость» и «доступность».

Контрольные вопросы

1. Обеспечение информационной безопасности информационных систем банков
2. Обеспечение информационной безопасности электронной коммерции
3. Обеспечение информационной безопасности учетной деятельности

Контрольные задания 6

Запустить программу «1С: Предприятие» и продемонстрировать возможности решения вопросы информационной безопасности на уровне пользовательского интерфейса и в режиме «Конфигуратор».

Экзаменационные вопросы

1. Прогресс информационных технологий и необходимость обеспечения безопасности
2. Основные понятия информатизации общества и информационной безопасности
3. Структура понятия «Информационная безопасность»
4. Субъекты и объекты информационной безопасности
5. Нормативно-правовое регулирование информационной безопасности
6. Типы международных организаций в сфере информационной безопасности
7. Направления работы крупных альянсов в сфере информационной безопасности
8. Понятие и особенности экономической информации как объекта безопасности
9. Перечень сведений, относящихся к коммерческой тайне
10. Перечень сведений, которые не могут составлять коммерческую тайну
11. Объекты банковской тайны
12. Статьи Уголовного кодекса о компьютерных преступлениях
13. Доктрина информационной безопасности РФ
14. Федеральный закон от №149-ФЗ «Об информации, информационных технологиях и о защите информации»
15. Федеральный закон от №63-ФЗ «Об электронной подписи»
16. Принципиальные подходы к обеспечению информационной безопасности
17. Сравнительная характеристика фрагментного и комплексного подхода к защите информации
18. Общие принципы обеспечения информационной безопасности
19. Специфические методы обеспечения информационной безопасности
20. Принципы построения системы информационной безопасности
21. Системный подход к защите информации
22. Требования к системе мер защиты информации
23. Принципы построения и особенности практической реализации системы защиты информации экономического субъекта
24. Механизм обеспечения информационной безопасности РФ в сфере экономики
25. Цели, задачи и функции системы защиты информации
26. Обеспечивающие компоненты системы защиты информации
27. Методы и средства обеспечения информационной безопасности
28. Сущность криптографических методов
29. Организационно-административные мероприятия обеспечения компьютерной безопасности
30. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения
31. Меры предупреждения и защиты от компьютерных преступлений
32. Информационные угрозы и их классификация
33. Действия и события, нарушающие информационную безопасность
34. Основные виды каналов утечки информации
35. Пути несанкционированного доступа к информации
36. Стратегия и тактика злоумышленника при несанкционированном доступе
37. Личностно - профессиональные характеристики сотрудников, способствующие реализации информационных угроз
38. Способы воздействия угроз на информационные объекты
39. Вредоносные программы, их виды
40. Признаки воздействия вирусов на компьютерную систему
41. Исторические аспекты компьютерных преступлений
42. Уголовно-правовая характеристика компьютерных преступлений,

43. Компьютерные преступления и их классификация
44. Субъекты компьютерных преступлений
45. Объективная сторона компьютерных преступлений
46. Уголовно-правовой контроль над компьютерной преступностью в РФ
47. Организация системы защиты информации экономических систем
48. Этапы построения системы защиты информации
49. Политика информационной безопасности
50. Способы практической реализации механизмов защиты информации
51. План построения системы защиты информации
52. Организация конфиденциального делопроизводства
53. Структура и функции службы информационной безопасности компании
54. Типы политики информационной безопасности
55. Оценка эффективности инвестиций в информационную безопасность
56. Обеспечение информационной безопасности автоматизированных банковских систем
57. Информационная безопасность электронной коммерции
58. Обеспечение компьютерной безопасности учетной информации
59. Информационная безопасность предпринимательской деятельности
60. Методика защиты электронной почты
61. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов
62. Электронная цифровая подпись и особенности ее применения
63. Защита информации в Интернете
64. Информационная безопасность пользователей мобильных устройств

Список рекомендуемых источников

1. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. – Режим доступа: http://znanium.com
2. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. – Режим доступа: http://znanium.com
3. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. – Режим доступа: http://znanium.com
4. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. – Режим доступа: http://znanium.com
5. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов, – 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с. Режим доступа: http://znanium.com
6. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014
7. Ясенев В.Н. Информационная безопасность в экономических системах: Учебно-методические пособие. – Н. Новгород, 2006
8. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации - 3-е изд., стер. – М.: Академия, 2008
9. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2009
10. www.cyberpol.ru Компьютерная преступность и способы борьбы.
11. www.iso27000.ru Информационный портал, посвященный вопросам управления информационной безопасностью.
12. www.itsec.ru Интернет-журнал «Информационная безопасность».
13. www.inside-zi.ru Информационно-методический журнал «Защита информации. Инсайд»
14. www.kaspersky.ru Лаборатория Касперского.