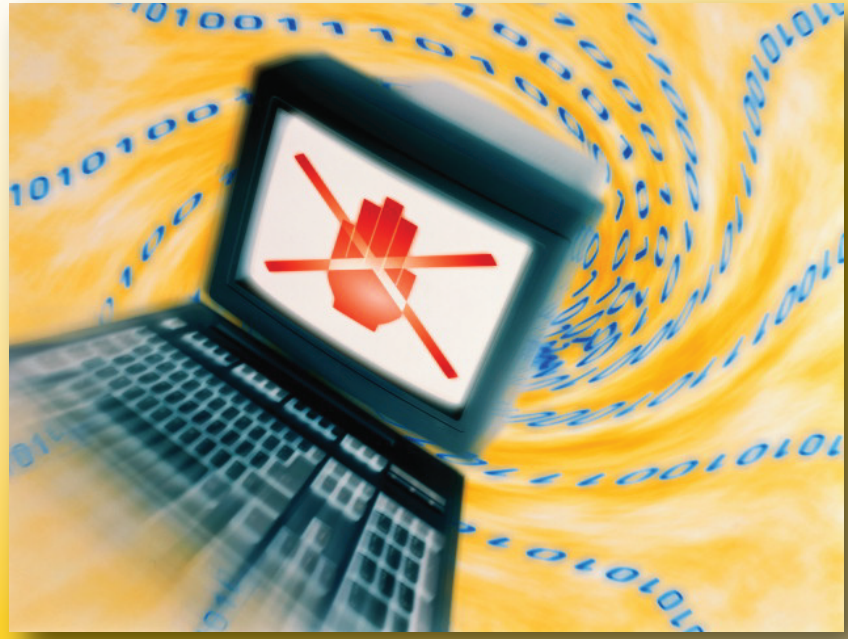
ТОЛЬЯТТИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Н.В. Ушмаева

ЗАЩИТА ИНФОРМАЦИИ

Учебно-методическое пособие



Министерство образования и науки Российской Федерации
Тольяттинский государственный университет
Институт математики, физики и информационных технологий
Кафедра «Информатика и вычислительная техника»

Н.В. Ушмаева

ЗАЩИТА ИНФОРМАЦИИ

Учебно-методическое пособие

Тольятти
Издательство ТГУ
2012

УДК 004.42
ББК 32.81
У95

Рецензенты:
к.т.н., доцент Поволжского государственного университета сервиса
В.Н. Будилов;
к.п.н., доцент Тольяттинского государственного университета
Е.В. Панюкова.

У95 Ушмаева, Н.В. Защита информации : учеб.-метод. пособие / Н.В. Ушмаева. – Тольятти : Изд-во ТГУ, 2012. – 56 с. : обл.

Учебно-методическое пособие «Защита информации» содержит методические рекомендации по изучению дисциплины, конспект лекций, практические задания, методические указания по выполнению контрольной работы, тесты.

Предназначено для студентов очной и заочной форм обучения направлений подготовки 080100.62 «Экономика», 230700.62 «Прикладная информатика» и 080801.65 «Прикладная информатика».

УДК 004.42
ББК 32.81

Рекомендовано к изданию научно-методическим советом Тольяттинского государственного университета.

ВВЕДЕНИЕ

В системе подготовки специалистов экономических специальностей одно из наиболее приоритетных направлений – формирование информационного мировоззрения. Дисциплина «Защита информации» является важной частью такой подготовки.

Цель данного учебно-методического пособия – помочь студентам заочной формы обучения в самостоятельном изучении дисциплины «Защита информации».

Структурно пособие состоит из следующих разделов:

- методические рекомендации по изучению дисциплины;
- конспект лекций;
- практикум;
- контрольная работа;
- тесты.

Методические рекомендации по изучению дисциплины включают цели и задачи дисциплины, рекомендации по изучению дисциплины, контрольные вопросы.

В разделе «Конспект лекций» рассматриваются теоретические вопросы об основах информационной безопасности, способах защиты информации, антивирусной защите, а также вопросы административно-правового обеспечения информационной безопасности.

В практикуме по дисциплине представлены практические задания и технология их выполнения по защите документов Microsoft Word, электронных таблиц и книг Microsoft Excel, баз данных Microsoft Access с помощью паролей, а также изучение криптографического закрытия информации на примере программной реализации симметричного алгоритма шифрования.

В разделе «Контрольная работа» в соответствии с номером варианта необходимо спроектировать демонстрационные слайды в программе Microsoft PowerPoint.

1. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ

1.1. Цель и задачи изучения курса

Цель изучения дисциплины «Защита информации» – дать студентам необходимые знания и умения в области информационной безопасности.

Задачи:

1) формирование теоретических знаний о способах защиты информации;
2) овладение приёмами в области создания систем защиты информации;
3) получение навыков самостоятельного использования прикладного программного обеспечения для защиты информации.

В результате обучения студент должен:

знать:

- вопросы административного и организационно-правового обеспечения защиты информации;
- основные системы защиты информации;
- основные методологические положения защиты информации;
- программно-аппаратные средства защиты компьютеров и программ;
- общие вопросы обеспечения информационной безопасности в компьютерных сетях;

уметь:

- ограничивать использование компьютера на основе раздельного доступа пользователей в операционную систему;
- использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов;
- организовать безопасную работу в Интернете и отправку почтовых сообщений в глобальной сети;

владеть навыками:

- защиты информации;
- использования в профессиональной деятельности средств обеспечения информационной безопасности;

- использования различных антивирусных программ и основы построения антивирусной защиты компьютерной системы организации;

обладать компетенциями:

- владения основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией, работы с информацией в глобальных компьютерных сетях;
- использования современных технических средств и информационных технологий для решения коммуникативных задач.

1.2. Методические рекомендации по изучению тем

Тема 1. Основные методы защиты информации

Цель – ознакомиться с основными способами и методами по защите информации.

Учебные вопросы

1. Аппаратные методы защиты.
2. Программные методы защиты.
3. Криптографическое шифрование информации.
4. Электронная цифровая подпись.
5. Резервное копирование.
6. Физические меры защиты.
7. Организационные мероприятия по защите информации.

Изучив данную тему, студент должен:

знать:

- основные способы и методы защиты информации;
- аппаратно-программные средства информационной безопасности;

уметь:

- использовать основные способы и методы защиты информации;
- применять программное обеспечение для построения информационной защиты;

иметь представление:

- о физических мерах в области информационной безопасности;
- организационных мероприятиях по защите информации.

При освоении темы необходимо:

- изучить учебный материал по теме 1;
- выполнить задание из Практикума 3.1;
- выполнить тест по теме 1;
- ответить на вопросы для самоконтроля.

Тема 2. Защита информации от компьютерных вирусов

Цель – ознакомиться с основными способами и методами защиты от компьютерных вирусов.

Учебные вопросы

1. Характеристика вирусов.
2. Классификация антивирусных программ.

Изучив данную тему, студент должен:

знать:

- характеристики вирусов и способы их обнаружения;
- антивирусные программы;

уметь:

- использовать антивирусные программы для защиты информации;
- устанавливать программное обеспечение для защиты информации от компьютерных вирусов;

иметь представление:

- о способах и методах обнаружения компьютерных вирусов;
- основных характеристиках и классификации вирусов;
- антивирусном программном обеспечении.

При освоении темы необходимо:

- изучить учебный материал по теме 2;
- выполнить задание из Практикума 3.2;
- выполнить тест по теме 2;
- ответить на вопросы для самоконтроля.

Тема 3. Правовые аспекты информационной безопасности

Цель – ознакомиться с правовыми и законодательными аспектами информационной безопасности.

Учебные вопросы

1. Законодательная система, обеспечивающая информационную безопасность в РФ.
2. Защита информации на примере некоторых статей УК.

Изучив данную тему, студент должен:

знать:

- законодательные и правовые акты по обеспечению информационной безопасности;
- степень административного и уголовного наказания за нарушения в области информационной безопасности;

уметь:

- использовать права и обязанности гражданина РФ при нарушении закона в области информационной безопасности;
- пользоваться информацией ограниченного доступа, в том числе конфиденциальной информацией.

При освоении темы необходимо:

- изучить учебный материал по теме 3;
- выполнить задание из Практикума 3.3;
- выполнить тест по теме 3;
- ответить на вопросы для самоконтроля.

1.3. Форма контроля

В ходе подготовки к зачету необходимо освоить теоретический материал, представленный в конспекте лекций данного учебно-методического пособия и в рекомендуемом библиографическом списке, ответить на все вопросы самоконтроля в конце каждого раздела, выполнить практические и тестовые задания, а также контрольную работу по своему варианту.

1.4. Вопросы к зачету

1. Перечислите основные причины, влияющие на развитие в области защиты информации.
2. Требования к системе информационной безопасности.
3. Основные каналы утечки информации.
4. Назовите основные методы защиты информации.
5. Аппаратные средства защиты.
6. Программные средства защиты.
7. Организационные средства защиты.
8. Электронно-цифровая подпись (ЭЦП).

9. Защита информации от несанкционированного доступа.
10. Программные методы защиты. На какие группы их можно разделить?
11. Что означает криптография?
12. Асимметричные и симметричные алгоритмы шифрования.
13. Защита информации от компьютерных вирусов.
14. Характеристика компьютерных вирусов.
15. Классификация антивирусных программ.
16. Законодательные основы информационной безопасности.
17. Основные направления правового обеспечения информационной безопасности.
18. Ответственность за преступления в области информационной безопасности.

2. КОНСПЕКТ ЛЕКЦИЙ

Тема 1. Основные методы защиты информации

Можно выделить три направления работ по защите информации:

1) теоретические исследования;
2) разработка средств защиты;
3) обоснование способов средств защиты в автоматизированных системах.

К настоящему времени разработано много различных средств, методов, мер и мероприятий, предназначенных для защиты информации, накапливаемой, хранимой и обрабатываемой в автоматизированных системах. Сюда входят аппаратные и программные средства, криптографическое закрытие информации, физические меры, организованные мероприятия, законодательные меры. Иногда все эти средства защиты делятся на технические и нетехнические. К техническим относятся аппаратные и программные средства и криптографическое закрытие информации, а к нетехническим – остальные средства, перечисленные выше.

Аппаратные методы защиты

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

- специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства;
- устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в запоминающем устройстве (ЗУ), которой принадлежат данные биты;
- схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.

Особую и получающую наибольшее распространение группу аппаратных средств защиты составляют устройства для шифрования информации (криптографические методы).

Программные методы защиты

К программным средствам защиты относятся специальные программы, которые предназначены для выполнения функций защиты и включаются в состав программного обеспечения систем обработки данных. Программная защита является наиболее распространенным видом защиты, чему способствуют такие положительные свойства данного средства, как универсальность, гибкость, простота реализации, практически неограниченные возможности изменения и развития и т. п. По функциональному назначению их можно разделить на следующие группы:

- идентификация технических средств (терминалов, устройств группового управления вводом-выводом, ЭВМ, носителей информации), задач и пользователей;
- определение прав технических средств (дни и время работы, разрешенные к использованию задачи) и пользователей;
- контроль работы технических средств и пользователей;
- регистрация работы технических средств и пользователей при обработке информации ограниченного использования;
- уничтожение информации в ЗУ после использования;
- сигнализация при несанкционированных действиях;
- вспомогательные программы различного назначения (контроль работы механизма защиты, проставление грифа секретности на выдаваемых документах).

Криптографическое шифрование информации

Криптография – наука о методах преобразования (шифрования) информации в целях ее защиты от незаконных пользователей. В современных криптосистемах шифр получают из исходного текста кодированием его символов, производимым на основе выбранного ***алгоритма шифрования и ключа***, указывающего, как именно происходит сопоставление символов исходного текста с символами кода.

Надежность шифрующего алгоритма, часто называемая его ***стойкостью*****,** определяется тем, насколько легко можно взломать шифр.

Принято считать, что надежность шифра определяется только ***секретностью*** используемого ключа, сам же алгоритм шифрования предположительно известен противнику. Стойкость используемых в настоящее время алгоритмов шифрования обеспечивается высокой вычислительной сложностью задачи выяснения значения ключа.

Существуют ***симметричные*** алгоритмы шифрования, в которых шифрование и дешифровка производятся с помощью одного и того же ключа, и ***асимметричные*** – требующие применения разных ключей.

Симметричные шифры строятся на алгоритме замены с помощью ключевого текста. Рассмотрим, например, следующий шифр. Пусть требуется зашифровать секретное сообщение «Операция начинается в воскресенье».

Все буквы русского алфавита пронумеровывают по порядку (от 1 до 33). Затем выбирают ключевое слово, например «Вологда», и подписывают его под сообщением с повторением, как показано ниже.

операциянаначинаетсяВвоскресенье
ВОЛОГДАВОЛОГДАВОЛОГДАВОЛОГДАВО

Чтобы получить шифрованный текст, номер очередной буквы сообщения складывается с номером соответствующей буквы ключа. Если полученная сумма больше числа 33, то из нее вычитается 33. В результате получают последовательность чисел, каждое из которых находится в диапазоне от 1 до 33. Вновь заменяя числа этой последовательности соответствующими буквами, получают шифрованный текст.

СЯСАДНЫЙВЭМЖМТБЗВЮОЁЖПФЪЭФХЙОЯФ

Математически данная процедура шифрования описывается операцией сложения по модулю, обратная ей (дешифровка) – операцией вычитания по модулю.

Сформируем расширенный алфавит как список всех символов, которые могут встречаться в шифруемых сообщениях. Количество символов расширенного алфавита обозначим через N. Тогда любой передаваемый текст можно рассматривать как последовательность $\{a_n\}$ чисел множества $A = \{0,1,2,...,N\}$. Выберем ключевую последовательность $\{c_n\}$ чисел множества A той же длины, что и передаваемый текст. Складывая по модулю N число a_n передаваемого текста с соответствующим числом c_n ключа

$$a_n + c_n \equiv (\text{mod } N),\ 0 \le b_n \le N\text{-}1,$$

получим последовательность $\{b_n\}$ знаков шифрованного текста. Чтобы его дешифровать, то есть получить передаваемый текст, можно воспользоваться тем же ключом:

$$a_n \equiv b_n - c_n\ (\text{mod } N),\ 0 \le a_n \le N\text{-}1.$$

У двух абонентов, находящихся в переписке, должен иметься один и тот же ключ.

Симметричные шифры обладают не очень высокой степенью стойкости, их раскрытие основано на использовании таблицы частот (буквы в естественном языке встречаются с разной частотой). Поэтому при практическом использовании подобных шифров применяют многократное шифрование, модификацию ключа и случайный выбор ключевых последовательностей.

К шифрам, предназначенным для закрытия информации в ЭВМ и автоматизированных системах, предъявляется ряд требований:

- достаточная стойкость (надежность закрытия);
- простота шифрования и расшифровки от способа внутри машинного представления информации;
- нечувствительность к небольшим ошибкам шифрования; возможность внутримашинной обработки зашифрованной информации;
- незначительная избыточность информации за счет шифрования и др.

В той или иной степени этим требованиям отвечают некоторые виды шифров замены, перестановки, гаммирования, а также шифры, основанные на аналитических преобразованиях шифруемых данных.

Шифрование заменой (иногда употребляется термин «подстановка») заключается в том, что символы шифруемого текста заменяются символами другого или того же алфавита в соответствии с заранее обусловленной схемой замены.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по какому-то правилу в пределах какого-то блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном и неповторяющемся порядке перестановки можно достигнуть достаточной для практических приложений в автоматизированных системах стойкости шифрования.

Шифрование гаммированием заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой гаммой. Стойкость шифрования определяется главным образом размером (длиной) неповторяющейся части гаммы. Поскольку с помощью ЭВМ можно генерировать практически бесконечную гамму, то данный способ считается одним из основных для шифрования информации в автоматизированных системах. Правда, при этом возникает ряд организационно-технических трудностей, которые, однако, не являются непреодолимыми.

Шифрование аналитическим преобразованием заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле). Можно, например, использовать правило умножения матрицы на вектор, причем умножаемая матрица является ключом шифрования (поэтому ее размер и содержание должны сохраняться в тайне).

Особенно эффективными являются комбинированные шифры, когда текст последовательно шифруется двумя или большим числом систем шифрования (например, замена и гаммирование, перестановка и гаммирование). Считается, что при этом стойкость шифрования превышает суммарную стойкость в составных шифрах.

Каждую из рассмотренных систем шифрования можно реализовать в автоматизированной системе либо программным путем, либо с помощью специальной аппаратуры. Программная реализация по сравнению с аппаратной является более гибкой и обходится дешевле. Однако аппаратное шифрование в общем случае в несколько раз производительнее. Это обстоятельство при больших объемах закрываемой информации имеет решающее значение.

Электронная цифровая подпись (ЭЦП)

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от под-

делки, 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. (Федеральный закон об ЭЦП, 2002 г.).

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме. (Федеральный закон об ЭЦП.)

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

ЭЦП для сообщения является последовательностью символов, зависящей как от самого сообщения, так и от некоторого секретного, известного только подписывающему субъекту ключа.

Схема цифровой подписи включает два алгоритма:

1) для вычисления;

2) для проверки подписи.

Вычисление подписи может быть выполнено только субъектом – владельцем сертификата ключа ЭЦП с использованием известного только ему ***закрытого*** ключа – уникальной последовательности символов.

Алгоритм проверки является общедоступным, чтобы проверить правильность подписи мог каждый. ***Для проверки используется открытый ключ.***

Как же работает технология цифровой подписи? Предположим, клиент (покупатель или магазин) хочет послать сообщение в банк, подписанное с помощью цифровой подписи. Применяя специальную хеш-функцию, он ***создает уникальным образом сжатый вариант исходного текста*** – дайджест, идентифицирующий текст так же, как отпечаток пальца – личность человека. Используемая хеш-функция гарантирует, что разные документы будут иметь разные электронные подписи и что даже самые незначительные изменения документа вызовут изменение его дайджеста. После этого клиент применяет к дайджесту своего сообщения особый криптографический алгоритм с помощью собственного закрытого ключа, и дайджест превращается в цифровую подпись, которая посылается по Интернету вместе с сообщением. Получив его, банк декодирует цифровую подпись посредством открытого ключа клиента, извлекает дайджест сообщения, применяет для сообщения ту

же хеш-функцию, что и клиент, получает свой, сжатый, вариант текста и сравнивает его с дайджестом, восстановленным из подписи. Если они совпадают, значит, подпись правильная, и сообщение действительно поступило от данного клиента. В противном случае сообщение либо отправлено из другого источника, либо было изменено после создания подписи – оно считается недействительным.

Резервное копирование

Резервное копирование информации заключается в хранении копии программ на носителе: стримере, гибких носителях, оптических и жестких дисках. На этих носителях копии программ могут находиться в нормальном (несжатом) или заархивированном виде. Резервное копирование проводится для сохранения программ от повреждений (как умышленных, так и случайных) и хранения редко используемых файлов.

При современном развитии компьютерных технологий требования к запоминающим устройствам в локальной сети растут гораздо быстрее, чем возможности. Наряду с геометрическим ростом емкости дисковых подсистем программам копирования на магнитную ленту за время, отпущенное на резервирование, приходится читать и записывать все большие массивы данных. Еще важнее то, что программы резервирования должны научить таким образом управлять большим количеством файлов, чтобы пользователям не было чересчур сложно извлекать отдельные файлы.

Физические меры защиты

Следующим классом в арсенале средств защиты информации являются физические меры. Это различные устройства и сооружения, а также мероприятия, которые затрудняют или делают невозможным проникновение потенциальных нарушителей в места, в которых можно иметь доступ к защищаемой информации. Чаще всего применяются нижеперечисленные меры:

- физическая изоляция сооружений, в которых устанавливается аппаратура автоматизированной системы, от других сооружений;
- ограждение территории вычислительных центров заборами на таких расстояниях, которые достаточны для исключения эффективной регистрации электромагнитных излучений и организации систематического контроля этих территорий;

– организация контрольно-пропускных пунктов у входов в помещения вычислительных центров или оборудование входных дверей специальными замками, позволяющими регулировать доступ в помещения;
– организация системы охранной сигнализации.

Организационные мероприятия по защите информации

Для защиты информации применяются организационные мероприятия. Это такие нормативно-правовые акты, которые регламентируют процессы функционирования системы обработки данных, использование ее устройств и ресурсов, а также взаимоотношение пользователей и систем таким образом, что несанкционированный доступ к информации становится невозможным или существенно затрудняется. Организационные мероприятия играют большую роль в создании надежного механизма защиты информации. Причины, по которым организационные мероприятия играют повышенную роль в механизме защиты, заключаются в том, что возможности несанкционированного использования информации в значительной мере обусловливаются нетехническими аспектами: злоумышленными действиями, нерадивостью или небрежностью пользователей или персонала систем обработки данных. Влияние этих аспектов практически невозможно избежать или локализовать с помощью аппаратных и программных средств, криптографического закрытия информации и физических мер защиты. Для этого необходима совокупность организационных, организационно-технических и организационно-правовых мероприятий, которая исключала бы возможность возникновения утечки информации подобным образом.

Основными организационными мероприятиями являются:
– мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров (ВЦ);
– мероприятия, осуществляемые при подборе и подготовке персонала ВЦ (проверка принимаемых на работу, создание условий, при которых персонал не хотел бы лишиться работы, ознакомление с мерами ответственности за нарушение правил защиты);
– организация надежного пропускного режима;
– организация хранения и использования документов и носителей: определение правил выдачи, ведение журналов выдачи и использования;

– контроль внесения изменений в математическое и программное обеспечение;
– организация подготовки и контроля работы пользователей.

Одно из важнейших организационных мероприятий – содержание в ВЦ специальной штатной службы защиты информации, численность и состав которой обеспечивали бы создание надежной системы защиты и регулярное ее функционирование.

Вопросы для самоконтроля

1. Основные направления и средства защиты информации.
2. Программные методы защиты. На какие группы их можно разделить?
3. Что означает криптография? Основные алгоритмы шифрования.
4. Назначение электронной цифровой подписи. Технология использования цифровой подписи.
5. Физические меры защиты.
6. Основные организационные мероприятия по информационной безопасности.

Тема 2. Защита информации от компьютерных вирусов

Защита информации от компьютерных вирусов в последнее время приобрела особую актуальность.

Компьютерные вирусы получили очень широкое распространение, и антивирусная борьба доставляет рядовому пользователю большую «головную боль». Поэтому важно понимать способы распространения и характер проявления вирусов, а главное – научиться применять антивирусные программы для эффективной борьбы с вирусами.

Характеристика вирусов

Вирус представляет собой самовоспроизводящуюся программу, которая способна внедрять свои копии в файлы, системные области, вычислительные сети и т. д. и приводить к нарушению нормального функционирования компьютера. Копии вирусной программы также сохраняют способность дальнейшего распространения. Вирусы классифицируются по следующим признакам: по среде обитания, способу заражения среды обитания, способу активации, деструктивным возможностям, особенностям алгоритма.

По ***среде обитания*** вирусы разделяют на файловые, загрузочные и сетевые. ***Файловые*** вирусы внедряются в файлы, чаще всего выполняемые, или файлы документов текстовых процессоров и рабочих книг табличных процессоров. ***Загрузочные*** вирусы внедряются в загрузочный сектор диска или в сектор системного загрузчика жесткого диска. ***Сетевые*** вирусы распространяются по компьютерной сети. Существуют также ***файлово-загрузочные*** вирусы, которые заражают файлы и загрузочные секторы.

Способ заражения среды обитания зависит от самой среды. В частности, тело файлового вируса может при заражении размещаться в конце, начале, середине или хвостовой (свободной) части последнего кластера файла. Достаточно просто реализуется внедрение вируса в конец файла типа сот. Наиболее сложна имплантация вируса в середину файла, поскольку для этого должна быть известна структура заражаемого файла, чтобы можно было внедриться, к примеру, в область стека. При внедрении загрузочного вируса (ввиду малых размеров среды обитания) используется размещение головы и тела вместо загрузочного сектора диска или сектора системного загрузчика, а хвост вируса и следующий за ним загрузочный сектор размещаются в других кластерах или секторах.

По ***способу активации*** вирусы подразделяют на резидентные и нерезидентные. ***Резидентный*** вирус при заражении оставляет в оперативной памяти резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения – файлам, загрузочным секторам и т. п. и внедряется в них. Резидентные вирусы сохраняют свою активность вплоть до выключения или перезагрузки компьютера. ***Нерезидентные*** вирусы являются активными ограниченное время и активизируются в определенные моменты, например, при запуске зараженных выполняемых программ или при обработке документов текстовым процессором. Некоторые нерезидентные вирусы оставляют в оперативной памяти небольшие резидентные программы.

По ***деструктивным возможностям*** вирусы разделяют на безвредные, неопасные, опасные и очень опасные. ***Безвредные*** вирусы проявляются только в том, что уменьшают объем памяти на диске в результате своего распространения. ***Неопасные*** вирусы, кроме отмеченного проявления, порождают графические, звуковые и другие эффекты. ***Опасные***

вирусы могут привести к нарушениям нормальной работы компьютера, например к неправильной печати документа. ***Очень опасные*** вирусы могут привести к уничтожению программ и данных, стиранию информации в системных областях памяти и даже приводить к выходу из строя движущихся частей жесткого диска при вводе в резонанс.

По ***особенностям алгоритмов*** различают следующие вирусы: спутники, черви, или репликаторы, паразитические, студенческие, невидимки или стелс-вирусы, призраки или мутанты. ***Вирусы-спутники*** файлы не изменяют, а для выполнимых программ (.exe) создают одноименные, которые при выполнении исходной программы запускаются первыми, а затем передают управление исходной выполняемой программе. ***Вирусы-черви*** распространяются в компьютерных сетях, вычисляют адреса сетевых компьютеров. ***Паразитические вирусы*** при распространении меняют содержимое дисковых секторов и файлов и, как следствие, легко обнаруживаются. ***Студенческие вирусы*** представляют собой простейшие, легко обнаруживаемые вирусы. ***Стелс-вирусы*** (от STEALTH – название проекта создания самолетов-невидимок) перехватывают обращение операционной системы к пораженным файлам и секторам дисков и подставляют незараженные участки диска, затрудняя тем самым их обнаружение. ***Вирусы-призраки*** представляют собой трудно обнаруживаемые вирусы, которые имеют зашифрованное с помощью алгоритмов шифровки-расшифровки тело вируса, благодаря чему две копии одного вируса не имеют одинаковых участков кода (сигнатур).

Классификация антивирусных программ

Антивирусными называются программы, предназначенные для защиты данных от разрушения, обнаружения и удаления компьютерных вирусов. Различают следующие разновидности антивирусных программ: фильтры, или сторожа; детекторы; доктора, или фаги; ревизоры; иммунизаторы, или вакцины.

Фильтр представляет собой резидентную программу, которая контролирует опасные действия, характерные для вирусных программ, и запрашивает подтверждение на их выполнение. К таким действиям относятся:

– изменение файлов выполняемых программ;
– размещение резидентной программы;

– прямая запись на диск по абсолютному адресу;
– запись в загрузочные секторы диска; форматирование диска.

Достоинством программ-фильтров является постоянное отслеживание ими опасных действий, повышающее вероятность обнаружения вирусов на ранней стадии их развития. С другой стороны, это же является и недостатком, так как приводит к отвлечению пользователя от основной работы для подтверждения запросов по подозрительным операциям.

Детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях. Различают детекторы универсальные и специализированные. Универсальные в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью причин искажения файлов. Специализированные детекторы выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы. Детектор, позволяющий обнаруживать несколько вирусов, называют полидетектором.

Доктором называют антивирусную программу, позволяющую обнаруживать и обезвреживать вирусы. При обезвреживании вирусов среда обитания может восстанавливаться или не восстанавливаться.

Полифаг – программа, предназначенная для обнаружения и уничтожения компьютерных вирусов (фаг – программа для обнаружения и уничтожения одного вируса). Как правило, полифаги используют базу данных, содержащую данные о вирусах, с которыми умеет бороться полифаг. Кроме того, современные полифаги, как правило, имеют эвристический анализатор, который позволяет обнаруживать вирусы, информация о которых не содержится в базе данных полифага. К их числу принадлежат получившие широкое распространение программы Doctor Web, Norton Antivirus, Virusscan, AVP, Антивирус Касперского и др. Основной нюанс их работы заключается в необходимости постоянного обновления базы данных, содержащей сведения о вирусах. При этом важно помнить, что каждый месяц появляется от 100 до 200 и более новых вирусов, поэтому программа, не обновленная несколько месяцев, может не обеспечить вашему ПК должную защиту от новых вирусов.

Ревизор представляет собой программу, запоминающую исходное состояние программ, каталогов и системных областей и периодически сравнивающую текущее состояние с исходным. Сравнение может выполняться по параметрам: длина и контрольная сумма файла и т. п. Достоинством ревизоров является их способность обнаруживать стелс-вирусы. К числу ревизоров относится хорошо известная программа ADinf.

Иммунизатор – резидентная программа, предназначенная для предотвращения заражения рядом известных вирусов путем их вакцинации. Суть вакцинации заключается в модификации программ или диска таким образом, чтобы это не отражалось на нормальном выполнении программ.

Вопросы для самоконтроля

1. Компьютерный вирус. Понятие.
2. По каким признакам можно определить, что компьютер заражен вирусом?
3. Способы заражения и среда обитания компьютерных вирусов.
4. Антивирусные программы. Классификация.

Тема 3. Правовые аспекты информационной безопасности

Законодательная система, обеспечивающая информационную безопасность в РФ

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (Закон РФ от 20.02.1995 г. № 24-ФЗ «Об информации, информатизации и защите информации»). Информация подпадает под нормы вещного права, что даёт возможность применять к информации нормы уголовного и гражданского права в полном объёме.

«К объектам гражданских прав относятся... информация, результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность)» (ст. 128, ч. 1 ГК РФ). Данная статья даёт возможность квалифицировать посягательства на сохранность и целостность информации как преступление против собственности. Для обеспечения чёткой правовой базы – применения к информации норм вещного права в Законе «Об информации» (ст. 5,

ч. 1) вводится понятие: «***документированная информация*** (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать».

Разрешение различных конфликтов в области информационных отношений на базе действующего законодательства возможно только для документированной информации (ст. 4.1, 6.1). Информационные ресурсы, т. е отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектами отношений физических, юридических лиц и государства, подлежат обязательному учёту и защите как материальное имущество собственника. Собственнику предоставляется право самостоятельно в пределах своей компетенции устанавливать режим защиты информационных ресурсов и доступа к ним (ст. 6.7).

Закон «Об информации» гласит: ***«Документированная информация*** ограниченного доступа по условиям её правового режима подразделяется на информацию, отнесённую к государственной тайне, и конфиденциальную» (ст. 10, ч. 2).

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ (ст. 2);

Персональные данные, которые входят в состав федеральных информационных ресурсов, совместного ведения, федерального и местного самоуправления, а также получаемые и собираемые негосударственными организациями, отнесены к категории конфиденциальной информации (ст. 11, ч. 1).

Не допускается сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, тайну переписки, телефонных переговоров и т. д. физического лица без его согласия, кроме как на основании судебного решения (ст. 11, ч. 1).

Основные направления правового обеспечения информационной безопасности

1. Права собственности, владения и распоряжения информацией.
2. Степень открытости информации.
3. Порядок отнесения информации к категории ограниченного доступа.

4. Организация работ по защите информации.
5. Государственное лицензирование деятельности в области защиты информации.

Защита информации на примере некоторых статей УК

Административно-правовая и уголовная ответственность за неправомерный доступ к компьютерной информации

Статья 272 УК предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло уничтожение, блокирование, модификацию, либо копирование информации, нарушение работы вычислительных систем.

Данная статья защищает право владельца на неприкосновенность информации в системе. Владельцем информационной вычислительной системы может быть любое лицо, правомерно пользующееся услугами по обработке информации как собственник вычислительной системы (ЭВМ, сети ЭВМ) или как лицо, приобретшее право использования компьютера.

Преступное деяние, ответственность за которое предусмотрено ст. 272, должно состоять в неправомерном доступе к охраняемой законом компьютерной информации. Это преступление носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств. Позволяет преодолевать установленные системы защиты, а также незаконно применять действующие пароли или маскировку под видом законного пользователя для проникновения в компьютер, хищения носителей информации, при условии, что были приняты меры по их охране, если это деяние повлекло уничтожение или блокирование информации.

Неправомерный доступ к компьютерной информации должен осуществляться умышленно. Совершая это преступление, лицо сознает, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность наступления указанных в законе последствий, желает и сознательно допускает их наступление, либо относится к ним безразлично.

Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК)

Статья 273 УК предусматривает уголовную ответственность за создание программ для ЭВМ или их модификацию, а равно использование таких программ или машинных носителей с такими программами. Это приводит к несанкционированному уничтожению, блокированию и модификации, либо копированию информации, нарушению работы информационных систем.

Статья защищает права владельца компьютерной системы на неприкосновенность находящейся в ней информации.

Под вредоносными программами согласно ст. 273 УК РФ понимаются программы, специально разработанные для нарушения нормального функционирования компьютерных программ.

Наиболее распространенными видами вредоносных программ являются широко известные компьютерные вирусы и логические бомбы.

Для привлечения к ответственности по статье 273 необязательно наступление каких-либо отрицательных последствий для владельца информации, достаточен сам факт создания программ или внесение изменений в существующие программы, заведомо приводящих к негативным последствиям, перечисленным в статье.

Уголовная ответственность по этой статье возникает уже в результате создания программы, независимо от того, использовалась эта программа или нет. По смыслу ст. 273 наличие исходных текстов вредоносных программ уже является основанием для привлечения к ответственности. Следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым. Это относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих соответствующую лицензию.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК)

Статья 274 УК устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред.

Статья защищает интерес владельца вычислительной системы относительно ее правильной эксплуатации.

Данная уголовная норма, естественно, не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально уполномоченным и доводиться до пользователей. Применение данной статьи невозможно для Интернета, ее действие распространяется только на локальные сети организаций.

Под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты.

Преступник, нарушивший правила эксплуатации, – это лицо, в силу должностных обязанностей имеющее доступ к компьютерной системе и обязанное соблюдать установленные для них технические правила. Преступник должен совершать свои деяния умышленно, он сознает, что нарушает правила эксплуатации, предвидит возможность или неизбежность неправомерного воздействия на информацию и причинение существенного вреда, желает или сознательно допускает причинение такого вреда или относится к его наступлению безразлично, что наиболее строго наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Ответственность за нарушения могут нести лица, достигшие 16 лет

***Статья* 272.** Предусматривает ответственность за несанкционированный доступ, если это повлекло уничтожение, блокировку, модификацию или копирование информации, нарушение работы вычислительных систем. Обычно несанкционированный доступ осуществляется умышленно (лишение свободы до двух лет 1 чел. и до пяти лет 2 чел., если группой лиц).

***Статья* 273.** Преступление, предусмотренное ч. 1 ст. 273, может быть совершено умышленно и максимальным наказанием является лишение свободы до трёх лет.

Статья 274. Обычно нарушение правил эксплуатации осуществляется умышленно. Преступление наказывается лишением права занимать определённые должности или заниматься определённой деятельностью на срок до пяти лет.

Вопросы для самоконтроля

1. Назовите основные направления правового обеспечения информационной безопасности.
2. Перечислите наиболее распространенные преступления в области информационных технологий.
3. Какова административная и уголовная ответственность за преступления в сфере информационных технологий?

3. ПРАКТИКУМ

3.1. Организация защиты файлов средствами текстового редактора Microsoft Word

Цель работы – освоить технологию организации парольной защиты файлов средствами текстового редактора Microsoft Word.

Задание

Создать документ, содержащий бланк официального письма, при условии, что:

– просмотр документа и создание на его основе других документов (конкретных писем) разрешены санкционированным пользователям с низким уровнем доступа LOW;
– изменение текста документа разрешено санкционированным пользователям с высоким уровнем доступа HIGH.

Организация защиты файлов средствами Microsoft Word

Существует несколько возможностей ограничения изменений в документе Word:

1) назначить документу пароль, предотвращающий открытие документа пользователем, не имеющим соответствующих полномочий;
2) назначить документу пароль, запрещающий запись, то есть позволяющий другим пользователям открывать документ только для чтения. Если кто-либо откроет предназначенный только для чтения документ и внесет в него изменения, сохранить этот файл он сможет только под другим именем;
3) рекомендовать другим пользователям работать с документом как с файлом, предназначенным только для чтения. Если кто-либо открывает этот документ как файл, предназначенный только для чтения, и вносит в него изменения, сохранить этот файл он сможет только под другим именем. Если же он открывает документ как обычный файл и вносит в него изменения, файл может быть сохранен под прежним именем;
4) назначить документу пароль, запрещающий изменение всего документа или отдельных разделов документа.

Внимание! Если после присвоения пароля он будет забыт, то невозможно будет ни открыть документ, ни снять с него защиту, ни восста-

новить данные из него. Поэтому следует составить список паролей и соответствующих им документов и хранить его в надежном месте.

Задание 1. Создать бланк исходящего письма организации, содержащий неизменяемые и изменяемые части.

1. Создать новый документ, содержащий следующий текст.

Тольяттинский государственный университет

г. Тольятти, ул. Белорусская, 14

2. Воспользовавшись панелью инструментов «***Формы***» (вызывается нажатием правой кнопки мыши на панели инструментов в области меню), вставить текстовые поля формы после слов «Исх – №», «от» и «/» для занесения исходящего номера письма, даты и фамилии исполнителя соответственно. Закрыть панель инструментов «Формы».

3. Разбить документ на три раздела: первый – содержащий шапку письма, второй – для текста письма и третий – включающий подпись исполнителя. Для этого вставить два разрыва раздела (после строки с исходящим номером и перед словом «Исполнитель»), оставив между ними пустую строку. Для вставки разрыва раздела необходимо в окне команды ***Вставка → Разрыв*** установить переключатель в позицию Новый раздел на текущей странице. Для просмотра вставленных границ разделов перейти к просмотру документа в обычном режиме, выполнив команду ***Вид → Обычный***. Если границы разделов установлены правильно, можно вернуться к режиму *«Разметка страницы»*.

4. Установить защиту документа, оставив возможность изменять значения полей формы и текст второго раздела. Для этого:

– выполнить команду ***Сервис → Защитить документ***;
– в появившемся окне «***Защита документа***» в группе «*Разрешить только указанный способ редактирования документа*» установить переключатель на позицию ввода данных в поля форм, в этом случае станет доступной кнопка ***Выбор разделов…***, открывающая окно «***Защита разделов***»;
– в окне «***Защита разделов***» выделить (отметить галочкой) только Раздел 1 и Раздел 3, нажать OK;
– в окне «***Защита документа***» на кнопке «*Да, включить защиту*» установить пароль HIGH на снятие защиты разделов. Ввести пароль HIGH еще раз в окне «*Подтверждение пароля*».

5. Проверить, что защита установлена, то есть можно вводить текст только в Раздел 2 и поля ввода формы из Раздела 1 и Раздела 3.

Задание 2. Установить защиту на разрешение записи документа. В этом случае, если документ открыт без пароля, он доступен в режиме «*только для чтения*».

6. В окне команды ***Сервис → Параметры***... выбрать вкладку ***Безопасность***. В группе *Параметры* совместного использования для данного документа ввести пароль HIGH в строку «пароль разрешения записи». Ввести пароль HIGH еще раз в окне «*Подтверждение пароля*».

Задание 3. Установить защиту на открытие документа. Проверить действие парольной защиты.

7. В окне команды ***Сервис → Параметры***... выбрать вкладку ***Безопасность***. В группе *Параметры* доступа к файлу ввести пароль LOW в строку «пароль для открытия файла». Нажать OK и ввести пароль LOW еще раз в окне «*Подтверждение пароля*».

8. Сохранить созданный документ под именем «**Письмо**» и закрыть документ.

9. Открыть «Письмо».

– в окне «*Пароль*» ввести пароль LOW для открытия файла «Письмо» и нажать OK;
– в следующем окне «*Пароль*» требуется ввести пароль для изменения документа «Письмо». Открыть документ в режиме «*только для чтения*». В этом случае после изменения документ может быть сохранен только под новым именем.

10. Внести в документ исходящий номер, дату, содержание письма и фамилию исполнителя.

11. Сохранить измененный документ.

Вызвать команду сохранения измененного документа (***Файл → Сохранить***). Будет открыто окно сохранения файла (как для команды ***Файл → Сохранить*** *как*...). Попытаться сохранить файл под тем же именем, для чего нажать кнопку *Сохранить*, ничего не меняя в окне сохранения. На экран будет выдано предупреждение о том, что данный файл открыт только для чтения.

Сохранить документ под именем «**Письмо 1**», документ не закрывать.

Задание 4. Снять парольную защиту с документа «Письмо 1» и рекомендовать к открытию его в режиме *«только для чтения»*.

12. В окне команды ***Сервис → Параметры***... выбрать вкладку ***Безопасность.*** В группе *Параметры доступа к файлу* удалить оба пароля и установить флажок «рекомендовать только для чтения», нажать OK.

13. Проверить, что при сохранении документа не требуется указание нового имени файла. Закрыть документ «Письмо 1».

14. Проверить, что открытие документа не требует введения никаких паролей. Исследовать реакции приложения Word 2003 при открытии и сохранении документа «Письмо 1».

Задание 5. Снять защиту с третьего раздела документа «Письмо».

15. Открыть документ «Письмо» с паролями на открытие LOW и на разрешение записи HIGH.

16. Снять защиту на изменение текста документа. Для этого вызвать команду ***Сервис → Снять защиту*** и указать в появившемся окне *«Снять защиту»* пароль HIGH.

17. Проверить, что все разделы документа доступны для внесения изменений.

18. Установить защиту для Раздела 1 с паролем HIGH.

19. В конец Раздела 3 вставить текущую дату командой ***Вставка → Дата и время***.

20. Сохранить документ «Письмо».

21. Показать документы «Письмо» и «Письмо 1» преподавателю.

3.2. Организация защиты файлов средствами Microsoft Excel

Цель работы – освоить технологию организации защиты файлов средствами электронной таблицы Microsoft Excel.

Задание

Создать книгу Excel, содержащую данные о сотрудниках, подразделениях организации и статистическую информацию о них, при этом:

- внесение изменений и просмотр данных о денежных начислениях разрешены только пользователям с высоким уровнем доступа (HIGH);
- просмотр прочих детальных данных о сотрудниках и подразделениях доступен пользователям со средним уровнем доступа (MEDIUM);

– пользователи с низким уровнем доступа (LOW) имеют доступ лишь к статистической информации о подразделениях организации.

Microsoft Excel обладает следующими возможностями защиты:

– ограничение доступа к отдельным элементам листа;
– ограничение возможности изменений для всей книги;
– ограничение доступа к книге с помощью пароля, запрашиваемого при открытии или сохранении книги, либо открытие книги посторонними в режиме «только для чтения».

Задание 1. Создать незащищенную книгу Excel.

1. Переименовать Лист1 в «**Статистика**», а Лист2 в «**Ведомость**». Удалить Лист3. Для этого щелкнуть правой кнопкой мыши по названию листа и выбрать соответствующее действие из контекстного меню.

2. На листе «Ведомость» создать таблицы следующих видов:

– в интервале ячеек A1:D11 создать таблицу, содержащую сведения о сотрудниках:

Сводная ведомость			
Фамилия	Разряд	Код подразделения	Начислено
Алексеева	14	2	
Иванов	17	1	
Петров	10	1	
Сидоров	17	2	
Смирнова	10	3	
Кукушкин	13	1	
Белова	15	3	
Давыдов	12	3	
Семенов	11	1	

– высчитать начисления в зависимости от разряда. Базовому разряду (десятому) начисляется 1300 руб. За каждую разрядную единицу сверх 10 начисляется по 110 руб. От полученной суммы берется 71 процент. Таким образом, для первой строки данных формула для расчета начислений будет иметь вид: **=0,71*(1300+110*(B3-10))**. Занести эту формулу в ячейку **D3**. Скопировать ее на диапазон **D3:D11;**

– в диапазоне ячеек **A13:C17** создать таблицу, содержащую данные о подразделениях организации:

Данные о подразделениях		
Код	Наименование	Руководитель
1	Общий отдел	Иванов
2	Отдел снабжения	Сидоров
3	Бухгалтерия	Белова

3. На листе «**Статистика**» создать форму вывода статистических данных:

– в ячейку **B3** занести текст «**Введите код отдела:**», в ячейку **B6** –«**Наименование подразделения:**», в ячейку **B8** – «**Руководитель**:», в ячейку **B10** – «**Численность сотрудников**:». Текст ячеек **B6, B8 и B10** выделить жирным;

– в ячейку E3 будет заноситься код подразделения. Если код не введен или определен неправильно, в ячейке B4 будет выдаваться подсказка «(**может быть равен 1, 2 или 3)**». Для этого в ячейку **B4** занести формулу:

=ЕСЛИ(ИЛИ(E3=1;E3=2;E3=3);"";"(может быть равен 1, 2 или 3);"");

– если код подразделения указан верно, в ячейке E6 будет выдаваться наименование подразделения. Для этого ввести в ячейку **E6** формулу

=ЕСЛИ(ИЛИ(E3=1;E3=2;E3=3);ВПР(E3;Ведомость!A15:C17;2;ЛОЖЬ);"")

– если код подразделения указан правильно, то в ячейке E8 будет выдаваться фамилия руководителя подразделения. Для этого ввести в ячейку **E8** формулу

=ЕСЛИ(ИЛИ(E3=1;E3=2;E3=3);ВПР(E3;Ведомость!A15:C17;3;ЛОЖЬ);"");

– если код подразделения указан правильно, то в ячейке E10 будет выдаваться численность сотрудников подразделения. Для этого ввести в ячейку **E10** формулу

=ЕСЛИ(ИЛИ(E3=1;E3=2;E3=3);СЧЁТЕСЛИ(Ведомость!C3:C10;E3);"");

– выделить ячейки E6, E8 и E10 жирным курсивом, шрифт – 11 кегль;

– выделить диапазон ячеек A5:C11 желтым цветом, диапазон A1:C4 – зеленым, ячейку E3 – оранжевым;

– сохранить книгу под именем «**Организация**».

Задание 2. Защитить необходимые элементы листов «Статистика» и «Ведомость» от изменений и просмотра.

4. На листе «Ведомость» скрыть столбец с данными о начислениях. Для этого установить курсор на любую ячейку столбца D и выполнить команду ***Формат → Столбец → Скрыть.***

5. Защитить лист «Ведомость». Для этого в окне команды ***Сервис → Защита*** установить флажки для всех строк группы *Защитить листы в отношении* и ввести пароль HIGH. Нажать OK, еще раз ввести пароль HIGH в появившемся окне подтверждения пароля и нажать OK.

6. На листе «Статистика» сделать доступным внесение данных в ячейку E3 после установки защиты. Для этого установить курсор на ячейке E3, в окне команды ***Формат → Ячейки*** выбрать вкладку *Защита*, снять флажок параметра *Защищаемая ячейка* и нажать OK.

7. Скрыть формулы. Выделить несмежные ячейки B4, E6, E8 и E10, для чего щелкнуть по ним мышью, удерживая клавишу CTRL. В окне команды ***Формат → Ячейки*** выбрать вкладку *Защита*, установить флажок параметра *Скрыть формулы* и нажать кнопку OK.

8. Установить защиту листа «Статистика» с паролем HIGH.

9. Проверить возможность внесения изменений в ячейку E3 и отсутствие такой возможности для остальных ячеек.

Задание 3. Ограничить возможность изменений структуры книги «Организация».

10. Скрыть лист «Ведомость»: перейти на лист «Ведомость» и выполнить команду ***Формат → Лист → Скрыть.***

11. Изменить размер окна книги так, чтобы была видна только выделенная цветом часть листа «Статистика». Расположить окно книги в центре экрана.

12. Установить защиту на изменение структуры книги и изменение размеров окна. В окне команды ***Сервис → Защита → Защитить книгу*** в группе *Защитить книгу* установить флажки, ввести пароль MEDIUM в группе пароль и в окне подтверждения пароля.

Задание 4. Задать пароль на открытие книги «Организация».

В окне команды ***Файл → Сохранить как…*** нажать кнопку-меню ***Сервис*** и выбрать пункт ***Общие параметры:***

– в появившемся окне ***Параметры сохранения*** ввести пароли LOW в строке *пароль для открытия файла* и HIGH в строке *пароль разрешения записи* соответственно. Нажать OK;

– в том же порядке ввести пароли в окнах подтверждения;

– в окне *Сохранение* документа нажать кнопку ***Сохранить***;

– закрыть книгу «Организация» с помощью команды ***Файл → Закрыть***.

Задание 5. Просмотреть информацию, содержащуюся в защищенной книге «Организация», последовательно применяя пароли разных уровней доступа.

13. Загрузить книгу «Организация» с низким уровнем доступа:

– открыть книгу «Организация». В окне ввода пароля доступа к защищенной книге ввести пароль LOW;

– в окне ввода пароля для разрешения записи пароль не вводить, а щелкнуть на кнопке *Только для чтения*;

– проверить невозможность изменения размеров и местоположения окна книги, невозможность просмотра других листов (команда ***Формат → Лист → Отобразить*** недоступна).

14. Просмотреть детальную информацию с листа «Ведомость», используя средний уровень доступа:

– снять защиту вида окна и структуры книги. Для этого выполнить команду ***Сервис → Защита → Снять защиту книги*** и ввести пароль MEDIUM;

– развернуть окно книги на весь экран;

– для просмотра листа «Ведомость» в окне команды ***Формат → Лист → Отобразить*** выбрать «Ведомость» и нажать OK.

15. Просмотреть информацию о денежных начислениях, используя высокий уровень доступа:

– перейти на лист «Ведомость»;

– проверить невозможность изменения содержимого листа, просмотра скрытых данных (столбца с суммами начислений) с помощью команды ***Формат → Столбец → Отобразить***;

– снять защиту листа, выполнив команду ***Сервис → Защита → Снять защиту листа*** и введя пароль HIGH;

– отобразить скрытый столбец D. Для этого выделить две любые смежные ячейки столбцов C и E, выполнить команду ***Формат → Столбец → Отобразить***.

16. Сохранить книгу MS Excel. Появится сообщение, что файл был открыт только для чтения и может быть сохранен под другим именем:

– ввести новое имя «**Организация _ защита _ снята**»;

– нажать кнопку ***Сервис*** и выбрать пункт ***Общие Параметры***, в появившемся окне окна *«Параметры сохранения»* удалить имеющийся пароль на открытие файла, выйти из окна, нажав OK;

– сохранить книгу под новым именем, нажав кнопку ***Сохранить*** в окне «*Сохранение документа*».

17. Показать книги **«Организация»** и **«Организация _ защита _ снята»** преподавателю.

3.3. Организация защиты баз данных средствами Microsoft Access

Цель работы – освоить технологию организации парольной защиты баз данных в Microsoft Access.

Задание

Создать базу данных, содержащую сведения о сотрудниках, подразделениях организации и статистическую информацию о них. Защитить базу данных шифрованием и паролем.

Организация защиты баз данных в MS Access

С помощью Microsoft Access можно использовать различные методы защиты баз данных. Для защиты базы данных, которая совместно используется лишь небольшой группой пользователей или на автономном компьютере, обычно достаточно установить парольную защиту и шифрование.

Установка пароля для открытия базы данных является простейшим способом защиты. После того как пароль установлен, при каждом открытии базы данных будет появляться диалоговое окно, в которое требуется ввести пароль. Только те пользователи, которые введут правильный пароль, смогут открыть базу данных. Этот способ достаточно надежен (Microsoft Access шифрует пароль, так что к нему нет прямого доступа при чтении файла базы данных), но он применяется только при открытии базы данных. После открытия базы данных все объекты становятся

доступными для пользователя. Для базы данных, которая совместно используется небольшой группой пользователей или на автономном компьютере, установка пароля обычно оказывается достаточной.

Шифрование базы данных защищает ее от несанкционированного просмотра с помощью служебных программ или текстовых редакторов. При шифровании базы данных ее файл сжимается, а работа с базой замедляется до 15 процентов. Шифрование незащищенной базы данных неэффективно, так как ее можно открыть в MS Access и получить полный доступ ко всем объектам. Шифрование защищенной базы данных – это хорошая защита от несанкционированного вмешательства при передаче по линии связи, хранении на дискете и т. п.

Задание 1. Подготовить созданную ранее книгу Excel «**Организация _ защита _ снята**» к экспорту данных в Access.

1. Открыть книгу Excel «**Организация _ защита _ снята**».

2. Задать имя «**Сотрудники**» диапазону листа «Ведомость», содержащему данные о сотрудниках организации:

– перейти на лист «Ведомость». Выделить диапазон ячеек **A2:D11**;

– выполнить команду ***Вставка → Имя → Присвоить***. В строке Имя появившегося окна «*Присвоение имени*» ввести слово «**Сотрудники**» и нажать OK.

3. Задать имя «**Подразделения**» диапазону **A14:C17** листа «Ведомость», содержащему данные о подразделениях организации.

4. Сохранить книгу и выйти из Excel.

Задание 2. Создать незащищенную базу данных о сотрудниках и подразделениях организации.

5. Создать новую базу данных Access, назвав ее «**Организация**».

6. В качестве исходных данных импортировать данные о сотрудниках с листа «Ведомость» книги Excel «Организация _ защита _ снята». Для этого:

– в окне базы данных выбрать объект *Таблицы* и выполнить команду ***Файл → Внешние данные → Импорт***;

– в окне «***Импорт***» выбрать из раскрывающегося списка тип файлов Microsoft Excel. Выбрать файл «**Организация _ защита _ снята**» и нажать кнопку ***Импорт***;

– в первом окне мастера импорта "*Импорт электронной таблицы*" установить переключатель на пункт *именованные диапазоны*, выбрать диапазон «Сотрудники» и нажать кнопку *Далее*;

– в следующем окне установить флажок параметра *Первая строка содержит заголовки столбцов* и нажать *Далее*;

– в следующем окне в группе *Данные* необходимо установить переключатель на пункт ***в новой таблице***, нажать *Далее*;

– в следующем окне мастера просмотреть макет таблицы и нажать *Далее;*

– в следующем окне мастера установить переключатель на пункт ***не создавать ключ*** и нажать *Далее*;

– в последнем окне мастера ввести «***Сотрудники***» в строке *Импорт* в таблицу и нажать кнопку *Готово*.

7. Аналогично пункту 6 импортировать данные о подразделениях из именованного диапазона «**Подразделения**» книги Excel «**Организация _ защита _ снята».**

8. Просмотреть полученные таблицы «***Сотрудники***» и «***Подразделения***».

9. Связать таблицу «***Подразделения***» с таблицей «***Сотрудники***» по полю «***Код***» (**связь 1 ко многим**).

10. Создать запрос с именем «***Статистика***», содержащий поля «*Наименование*» и «*Руководитель*» из таблицы «***Подразделения***». Поле «*Фамилии*» из таблицы «***Сотрудники***» с группировкой по *наименованиям подразделений:*

– по полю «*Фамилия*» должно подсчитываться количество сотрудников, для чего необходимо выбрать функцию **Count** в групповых операциях.

11. На основе запроса «*Статистика*» создать форму «*Статистика*». Заголовок последнего поля изменить с «**Count _ Фамилия**» на «***Численность сотрудников***».

12. Не выходя из MS Access, закрыть базу данных «**Организация**».

Задание 3. Защитить базу данных для монопольного доступа.

13. Зашифровать базу:

– не открывая базы данных, выполнить команду ***Сервис → Защита → Шифровать → Дешифровать*;**

– в появившемся окне выбрать базу данных **«Организация»** и нажать *OK;*

– в следующем окне в строку *Имя файла* ввести имя новой (зашифрованной) базы данных «**Организация _ шифр**» и нажать кнопку *Сохранить*.

14. Защитить открытие зашифрованной базы паролем:

– выполнить команду ***Файл → Открыть***. В окне *«Открытие файла базы данных»* выбрать имя базы "**Организация _ шифр**";

– щелкнуть мышью на указателе выпадающего списка (стрелочка вниз) кнопки *Открыть* и выбрать из списка пункт *Монопольно*;

– выполнить команду ***Сервис → Защита → Задать пароль базы данных.*** В окне ввода пароля дважды ввести пароль HIGH и нажать *OK*.

15. Закрыть базу «Организация _ шифр» и вновь открыть ее (в окне открытия базы данных просто щелкнуть на кнопке *Открыть*), воспользовавшись паролем HIGH.

3.4. Элементы криптографии. Симметричный алгоритм шифрования

Цель работы – освоить технологию программирования алгоритма шифрования.

Задание

Изучить симметричный алгоритм шифрования (на примере программы **cript.pas**).

Программа содержит две процедуры – шифрование текста и дешифровка текста, зашифрованного с помощью симметричного алгоритма.

Разберем текст программы. В программе объявлены глобальные переменные:

- ***text_in –*** строка, предназначенная для шифрования;
- ***text_out*** – строка зашифрованного текста,
- ***cript_st*** – ключевая строка.

Объявлена переменная ***alf_st*,** строка, в которой перечислены все допустимые символы, которые могут содержаться в шифруемой строке и ключевом слове.

До начала работы процедур шифрования или дешифровки нам надо выполнить подготовительную работу. Имея доступ к строке до-

пустимых символов, мы можем любому числу ***i*** от 1 до длины строки ***alf_st*** поставить в соответствие допустимый символ ***alf_st[i].*** Надо организовать возможность получения обратной зависимости. Для этого заведем массив ***alf2num*** с элементами типа **integer**, в котором индексами являются символы с кодами от 1 до 255. Заполним этот массив.

```
var
 text_in, text_out, cript_st, alf_st: string;
 alf2num: array [chr(1).. chr(255)] of integer;
 i,ln: integer;
begin
   alf_st:='ячсмитьбюфывапролджэйцукенгшщзхъЯЧСМИТЬБЮФЫ
ВАПРОЛДЖЭЙЦУКЕНГШЩЗХЪ 1234567890.,+=)(-!?';
 ln:=length(alf_st);
 for i:=1 to ln do begin
 alf2num[alf_st[i]]:=i;
 end;
```

Теперь, когда подготовительная работа окончена, рассмотрим процедуру шифрования текста. В процедуру передается шифруемая строка **text_in** и ключевая строка **cript_st.**

```
Procedure cript_in (criptin, key_text: string);
Var
 cript_text, textout: string;
 d, i, text_len: integer;
begin
 text_len:=length(criptin); {Определяем длину строки для шифрования}
 cript_text:=key_text;
```

{Формируем ключевую строку путем повторения ключевого слова, пока ее длина не превысит длину шифруемой строки}

```
 while length(cript_text)<=text_len do begin
 cript_text:= cript_text+key_text;
 end;
 textout:='';
```

{Вычисляем по очереди каждый зашифрованный символ. Для этого определяем номера очередных символов шифруемой и ключевой строк в строке допустимых символов, складываем их и ищем остаток от

деления полученного числа на длину алфавита. Таким образом, мы получаем число, лежащее в диапазоне от 1 до длины алфавита. Находим символ, соответствующий этому числу, и записываем его в результирующую (зашифрованную) строку}

```
for i:=1 to text_len do begin
if alf2num[criptin[i]]=-1 then begin
writeln('Недопустимый символ', criptin[i]);
exit;
end;
d:=alf2num[criptin[i]]+alf2num[cript_text[i]];
d:= d mod ln;
textout:= textout+alf_st[d];
end;
```

writeln(textout); {процедура выводит на экран зашифрованный текст}

end;

Процедура дешифровки очень похожа на процедуру шифрования, с той лишь разницей, что вместо складывания номеров символов исходной и ключевой строк мы ищем их разность и затем, если получается отрицательный ответ, прибавляем к нему длину алфавита, с тем чтобы результирующее число находилось в диапазоне между 1 и длиной алфавита.

```
Procedure cript_out (criptout, key_text: string);
Var
cript_text, textin: string;
d, i, text_len: integer;
begin
```

text_len:=length(criptout); {Определяем длину строки для шифрования}

```
cript_text:=key_text;
```

{Формируем ключевую строку путем повторения ключевого слова, пока ее длина не превысит длину шифруемой строки}

```
while length(cript_text)<=text_len do begin
cript_text:= cript_text+key_text;
end;
textin:='';
```

```
for i:=1 to text_len do begin
if alf2num[criptout[i]]=-1 then begin
writeln('Недопустимый символ', criptout[i]);
exit;
end;
d:=alf2num[criptout[i]]-alf2num[cript_text[i]];
d:= d mod ln;
textin:= textin+alf_st[d];
end;
```

```
writeln(textin);
```
{процедура выводит на экран расшифрованный текст}

```
end;
```

Приведем полный текст программы

```
Program cript;
var
text_in, text_out, cript_st, alf_st: string;
alf2num: array [chr(1).. chr(255)] of integer;
i,ln: integer;
Procedure cript_in (criptin, key_text: StType);
Var
cript_text, textout: string;
d, i, text_len: integer;
begin
text_len:=length(criptin);
```
{Определяем длину строки для шифрования}

```
cript_text:=key_text;
```
{Формируем ключевую строку путем повторения ключевого слова, пока ее длина не превысит длину шифруемой строки}

```
while length(cript_text)<=text_len do begin
cript_text:= cript_text+key_text;
end;
textout:='';
for i:=1 to text_len do begin
```
{Цикл, в котором происходит шифрование}

{Проверим строку на наличие символов, не входящих в заданный алфавит. Если такие встретятся, программа выдает сообщение об ошибке и выходит из процедуры}

```
if alf2num[criptin[i]]=0 then begin
writeln('Недопустимый символ', criptin[i]);
exit;
end;
d:=alf2num[criptin[i]]+alf2num[cript_text[i]];
d:= d mod ln;
textout:= textout+alf_st[d];
end;
 writeln(textout); {процедура выводит на экран зашифрованный текст}
end;
Procedure cript_out (criptout, key_text: StType);
Var
cript_text, textin: string;
d, i, text_len: integer;
begin
 text_len:=length(criptout); {Определяем длину строки для шифрования}
cript_text:=key_text;
{Формируем ключевую строку путем повторения ключевого слова, пока ее длина не превысит длину шифруемой строки}
while length(cript_text)<=text_len do begin
cript_text:= cript_text+key_text;
end;
textin:='';
for i:=1 to text_len do begin
if alf2num[criptout[i]]=0 then begin
writeln('Недопустимый символ ', criptin[i]);
exit;
end;
d:=alf2num[criptout[i]]-alf2num[cript_text[i]];
d:= d mod ln;
textin:= textin+alf_st[d];
end;
 writeln(textin); {процедура выводит на экран расшифрованный текст}
```

```
end;
begin
 alf_st:='ячсмитьбюфывапролджэйцукенгшщзхъЯЧСМИТЬБЮФЫ
 ВАПРОЛДЖЭЙЦУКЕНГШЩЗХЪ 1234567890.,+=)(-!?';
 ln:=length(alf_st);
 for i:=1 to 255 do begin
 alf2num[alf_st[i]]:=-1;
 end;
 for i:=1 to ln do begin
 alf2num[alf_st[i]]:=i;
 end;
 Writeln('Введите ключевое слово');
 Readln(cript_st); {Читаем ключевое слово}
 Writell('Введите строку, подлежащую шифрованию');
 Readln(text_in); {Читаем строку, которую надо зашифровать}
{шифрование выполняется, ответ выводится на экран}
 Cript_in(text_in, cript_st);
 Writeln('Введите текст для расшифровки');
 Readln(text_out); {Читаем текст для расшифровки}
{расшифровка выполняется, ответ выводится на экран}
 Cript_out(text_out, cript_st);
 Readln;
End.
```

4. КОНТРОЛЬНАЯ РАБОТА

Цели работы:

– научиться на практике применять знания, полученные при изучении теоретического материала по теме «Защита информации»;
– научиться проектировать демонстрационные слайды в программе презентаций MS PowerPoint.

Общие рекомендации по выполнению контрольной работы

В соответствии с **номером варианта** каждый студент поэтапно проектирует демонстрационные слайды в программе презентаций MS PowerPoint. Номер варианта соответствует порядковому номеру в списке группы.

В процессе проектирования можно условно выделить три этапа:

1) подбор теоретического материала для демонстрационных слайдов;
2) подготовка материала к компьютерной реализации и выбор стиля оформления;
3) проектирование демонстрационных слайдов в программе презентаций MS PowerPoint.

Представление результатов выполнения контрольной работы

Результатом выполнения контрольной работы является **файл презентации в формате Microsoft PowerPoint**. Презентация представляется преподавателю на зачетной неделе. **Защита контрольной работы** проходит в форме демонстрации. Для подготовки к защите следует ответить на вопросы самоконтроля данного методического пособия. Контрольная работа будет зачтена**,** если выполнена в полном объеме и в установленные сроки.

Варианты заданий

1. Информационная безопасность (ИБ) и ее составляющие.
2. Угрозы безопасности информации и их классификация.
3. Основные виды защищаемой информации.
4. Проблемы информационной безопасности в мировом сообществе.
5. Законодательные и иные правовые акты РФ, регулирующие правовые отношения в сфере информационной безопасности и защиты государственной тайны.
6. Система органов обеспечения информационной безопасности в РФ.

7. Административно-правовая ответственность в информационной сфере.
8. Уголовная ответственность в информационной сфере.
9. Защита от несанкционированного вмешательства в информационные процессы.
10. Организационные меры, инженерно-технические и иные методы защиты информации, в том числе сведений, составляющих государственную тайну.
11. Защита информации в локальных и глобальных компьютерных сетях.
12. Антивирусная защита.
13. Специфика обработки конфиденциальной информации в компьютерных системах.
14. Классификация вирусов.
15. Криптографические методы защиты информации.
16. Защита информации в банковской сфере.
17. Электронно-цифровая подпись.
18. Принципы построения системы информационной безопасности объекта.
19. Требования к системе информационной безопасности.
20. Порядок действий по обеспечению безопасности коммерческой тайны.
21. Законодательные основы обеспечения информационной безопасности.
22. Основные направления правового обеспечения информационной безопасности.
23. Ответственность за преступления в области информационной безопасности.
24. Информационные ресурсы ограниченного доступа.
25. Обеспечение защищенности от внешних и внутренних угроз в сфере формирования, распространения и использования информационных ресурсов.
26. Обеспечение защищенности информационных ресурсов, составляющих государственную тайну.
27. Симметричные и асимметричные алгоритмы шифрования.
28. Классификация антивирусных программ.
29. Характеристика вирусов.
30. Обеспечение защищенности от внешних и внутренних угроз в банковской сфере.

5. ТЕСТЫ

5.1. Тестовые задания по теме 1

1. Криптография – это наука...
a) об обеспечении секретности передаваемых сообщений
b) видах вирусов в графических файлах
c) вирусах в компьютерных сетях
d) обеспечении техники безопасности

2. Какая информация по своему правовому режиму не является информацией с ограниченным доступом?
a) конфиденциальная
b) частная
c) информация о личности
d) массовая информация

3. К аппаратным средствам защиты не относятся
a) электронные устройства
b) электронно-механические устройства
c) электронно-оптические устройства
d) вспомогательные программы различного назначения

4. К физическим мерам защиты не относятся
a) ограничение территории забором
b) организация систем охранной сигнализации
c) организация контрольно-пропускных пунктов
d) сетевые фильтры

5. К каким методам защиты относится парольная защита?
a) программным
b) физическим
c) инструментальным
d) аппаратным

6. Методом защиты информации не является
a) резервное копирование
b) криптография
c) дефрагментация диска
d) уничтожение информации в ЗУ после использования

7. Для защиты электронного документа от подделки с помощью электронно-цифровой подписи используется
a) только закрытый ключ
b) только открытый ключ
c) закрытый и открытый ключ

8. Сжатый образ исходного текста обычно используется
a) в качестве ключа для шифрования текста
b) для создания электронно-цифровой подписи
c) как открытый ключ в симметричных алгоритмах
d) как результат шифрования текста для его отправки по незащищенному каналу

9. В основные методы защиты информации входит
a) регистрация и учет пользователей
b) блокировка компьютера
c) архивация файлов
d) резервное копирование

10. К техническим средствам защиты не относятся
a) аппаратные
b) программные
c) криптография
d) организационные

5.2. Тестовые задания по теме 2

1. Компьютерный вирус – это
a) программа любого языка ЭВМ
b) неполадки в компьютере
c) самовоспроизводящаяся программа
d) вид неисправности

2. В какие файлы чаще всего внедряются файловые вирусы?
a) документов текстовых процессоров
b) выполняемые
c) рабочих книг табличных процессоров
d) графические

3. Нерезидентные вирусы являются активными

a) в любые моменты времени
b) в определенные моменты времени
c) ограниченное время
d) постоянное время

4. Не является антивирусной программой

a) фильтры
b) детекторы
c) полифаг
d) монофаг

5. Каких не бывает компьютерных вирусов?

a) загрузочных
b) файловых
c) макровирусы
d) драйверных

6. Наиболее просто реанимировать внедрение вируса

a) в начало файла
b) середину файла
c) конец файла
d) не имеет значения

7. Фильтр представляет собой резидентную программу, которая...

a) обнаруживает и уничтожает компьютерные вирусы
b) контролирует опасные действия, характерные для вирусных программ
c) обнаруживает компьютерные вирусы
d) распознает вирусы

8. Детекторы обеспечивают поиск и обнаружение вирусов

a) в оперативной памяти
b) постоянном запоминающем устройстве
c) внешней памяти
d) кэш-памяти

9. Для блокировки атак используются

a) компоненты MS Office
b) антивирусные программы

c) браузер
d) архиваторы

10. Какие из перечисленных ниже действий не могут привести к вирусной атаке?
a) получение файла по электронной почте
b) создание нового документа MS Office
c) установка на компьютер новой программы с зараженного диска
d) получение информации из Интернета

5.3. Тестовые задания по теме 3

1. Какие нарушения предусматривают уголовную ответственность в сфере информационных технологий?
a) неправомерный доступ
b) использование и распространение вредоносных программ
c) нарушение правил эксплуатации ЭВМ
d) все перечисленное

2. Какая документированная информация является информацией ограниченного доступа?
a) массовая
b) конфиденциальная
c) открытая
d) публичная

3. Защита юридической значимости электронных документов необходима при использовании информационных объектов, содержащих
a) дипломные проекты
b) приказы
c) финансовые документы
d) проекты зданий

4. Выберите из списка основные направления правового обеспечения информационной безопасности
a) права собственности, владения и распоряжения информацией
b) степень открытости информации
c) порядок отнесения информации к категории ограниченного доступа
d) тиражирование и распространение массовой информации

5. Какие правовые санкции можно применить, если было установлено на компьютер инфицированное программное обеспечение без антивирусной проверки?

a) лишается права занимать определенные должности на срок до пяти лет
b) ограничивается штрафом
c) лишением свободы на срок до двух лет
d) при таких нарушениях нет наказания

6. Защита юридической значимости электронных документов необходима при использовании информационных объектов, содержащих

a) дипломные проекты
b) курсовые работы
c) приказы, финансовые документы
d) проекты зданий

7. Какая из перечисленных статей УК предусматривает ответственность за неправомерный доступ к компьютерной информации?

a) статья 272
b) статья 273
c) статья 274
d) статья 275

8. Разработчика компьютерных вирусов обычно называют

a) модератор
b) тьютор
c) хакер
d) маклер

Заключение

Во все времена информация играла огромную роль в жизни каждого человека. Все многообразие информационных потоков и источников законодательство Российской Федерации делит на открытую информацию и информацию ограниченного доступа. И каждый вид представленной информации нуждается в защите (как авторское право, так и защита от несанкционированного доступа), в обеспечении сохранности, подлинности, достоверности.

Переход к рыночным отношениям, развитие предпринимательства и конкурентных отношений вызывают необходимость правовой защиты информации, разглашение которой может нанести ущерб субъектам хозяйствования.

Данное учебно-методическое пособие посвящено проблемам обеспечения информационной безопасности и методам их решения применительно к конфиденциальной информации.

Библиографический список

1. Партыка, Т.Л. Информационная безопасность : учеб. пособие для сред. проф. образования / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ : ИНФРА-М, 2005. – 367 с.
2. Партыка, Т.Л. Информационная безопасность : учеб. пособие для сред. проф. образования / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ : ИНФРА-М, 2004. – 367 с.
3. Прокофьев, И.В. Защита информации в информационных интегрированных системах : учеб. для вузов / И.В. Прокофьев ; ред. кол. : В.Н. Азаров [и др.]. – М. : Европ. центр по качеству, 2002. – 137 с.
4. Защита информации : метод. указания / Н.В. Ушмаева [и др.]. – Тольятти : ТГУ, 2007. – 70 с.
5. Лекции по защите информации [Электронный ресурс] – Режим доступа: http://www.studfiles.ru/
6. Федеральный закон «Об информации, информатизации и защите» [Электронный ресурс] – Режим доступа: http://www.securitylab.ru/
7. Информационная безопасность [Электронный ресурс] – Режим доступа: http://dehack.ru/

Глоссарий

Алгоритм – точное предписание исполнителю выполнить определенную последовательность действий для достижения поставленной цели за конечное число шагов.

Антивирусная программа – обслуживающая программа, предназначенная для защиты данных от разрушения, обнаружения и удаления компьютерных вирусов.

Асимметричные – алгоритмы шифрования, в которых шифрование и дешифровка производятся с применением разных ключей.

Вирус – самовоспроизводящаяся программа, которая способна внедрять свои копии в файлы, системные области, вычислительные сети и т. д. и приводить к нарушению нормального функционирования компьютера.

Детекторы – обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях.

Доктор – антивирусная программа, позволяющая обнаруживать и обезвреживать вирусы. При обезвреживании вирусов среда обитания может восстанавливаться или не восстанавливаться.

Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ (ст. 2).

Иммунизатор – резидентная программа, предназначенная для предотвращения заражения рядом известных вирусов путем их вакцинации.

Криптография – наука о методах преобразования (шифрования) информации в целях ее защиты от незаконных пользователей

Полифаг – программа, предназначенная для обнаружения и уничтожения компьютерных вирусов (фаг – программа для обнаружения и уничтожения одного вируса). Как правило, полифаги используют базу данных, содержащую данные о вирусах, с которыми умеет бороться полифаг.

Ревизор – программа, запоминающая исходное состояние программ, каталогов и системных областей и периодически сравнивающая текущее состояние с исходным.

Симметричные алгоритмы шифрования – шифрование и дешифровка в них производятся с помощью одного и того же ключа.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного 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. (Федеральный закон об ЭЦП, 2002 г.)

СОДЕРЖАНИЕ

Учебное издание

Ушмаева Нина Витальевна

ЗАЩИТА ИНФОРМАЦИИ

Учебно-методическое пособие

Технический редактор *З.М. Малявина*
Корректор *Г.В. Данилова*
Вёрстка: *Л.В. Сызганцева*
Дизайн обложки: *Г.В. Карасева*

Подписано в печать 21.96.2012. Формат 60×84/16.
Печать оперативная. Усл. п. л. 3,25.
Тираж 50 экз. Заказ № 1-41-11.

Издательство Тольяттинского государственного университета
445667, г. Тольятти, ул. Белорусская, 14