ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА – ЮГРЫ

БУ ВО «СУРГУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра автоматизированных систем обработки информации и управления

ЗАЩИТА ИНФОРМАЦИИ

Учебно-методическое пособие

Сургут
Издательский центр СурГУ
2019

УДК 004.056(072)
ББК 32.973я73
З-402

Печатается по решению
редакционно-издательского совета СурГУ

Рецензенты:
к. ф.-м. н., зав. кафедрой прикладной математики СурГУ
А. В. Гореликов;
к. т. н., ст. преподаватель кафедры автоматизированных систем
обработки информации и управления СурГУ **Е. А. Яценко**

Защита информации : учеб.-метод. пособие. / сост. Т. В. Гавриленко [и др.]. – Сургут : ИЦ СурГУ, 2019. – 63 с.
З-402

Учебно-методическое пособие разработано в соответствии с ФГОС ВО по направлениям подготовки 27 03 04 Управление в технических системах, 09 03 01 Информатика и вычислительная техника, 01 03 02 Прикладная математика и информатика, рабочей программой дисциплины «Защита информации» и предназначено для студентов бакалавриата.

Пособие содержит теоретический материал, описание и порядок выполнения практических работ.

УДК 004.056(072)
ББК 32.973я73

ОГЛАВЛЕНИЕ

Введение 4
Правовые основы защиты информации и информационных технологий 4
Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации» 10
Основные положения Федерального закона «О персональных данных» 18
Права на результаты интеллектуальной деятельности и средства индивидуализации 21
Криптография. Классификация криптографических систем 24
Практические задания 30
Задание 1. Алгоритм шифрования 30
Задание 2. Алгоритм шифрования с ключом 32
Задание 3. Симметричный алгоритм шифрования 34
Задание 4. Асимметричный алгоритм шифрования 39
Задание 5. Хеш-функция 41
Задание 6. Защита программ от несанкционированного доступа 46
Задание 7. Пространство имен Gryptography.NET 47
Контрольные вопросы по курсу 49
Словарь терминов 52
Список литературы 57
Приложение 59

ВВЕДЕНИЕ

Учебно-методическое пособие разработано в соответствии с рабочей программой дисциплины «Защита информации», предназначено для студентов бакалавриата, обучающихся по направлениям подготовки 27 03 04 Управление в технических системах, 09 03 01 Информатика и вычислительная техника, 01 03 02 Прикладная математика и информатика.

Пособие состоит из трех разделов. В первом разделе рассмотрены основные законодательные акты, связанные с защитой информации; проблемы защиты информации и методы их решения.

Во втором разделе дана краткая история развития криптографии и классификация криптографических систем, базовые понятия, связанные с криптографической защитой данных.

Третий раздел содержит задания к практическим работам, методические указания по их выполнению, вопросы для самопроверки, словарь терминов по теме.

Приложение к учебно-методическому пособию содержит описание видов вредоносных компьютерных программ.

ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

На протяжении практически всего периода развития вычислительных и информационных систем вопросы защиты информации становятся все более и более острыми: постоянно появляются сообщения о хакерских атаках, новом вредоносном программном обеспечении и уязвимости тех или иных аппаратных и программных комплексов (прил.). Для защиты информации, препятствования распространению незаконного контента и вредоносных программ создаются новые методы и средства защиты информации, изменяется международное и государственное право.

В области защиты информации действуют морально-этические и нормативно-правовые нормы. Нормативно-правовую базу формирует международное сообщество, государство, различные ведомственные структуры, организации и компании. Любой пользователь, вовлеченный в информационные процессы, должен знать основные нормативно-правовые акты, регулирующие его деятельность в области информатизации и защиты информации.

Защита информации является одним из ключевых компонентов информатизации и создания цифрового общества. При этом необходимо защищать не только информацию от несанкционированного доступа, незаконного использования, но и пользователей от различной вредоносной информации. Развитие информационного общества и цифровизация всех сфер человеческой деятельности приводит к тому, что информация становится самым дорогим и востребованным продуктом. Взрывное развитие сетей передачи данных позволило кардинально изменить объем носителей информации, методы доступа и скорость обмена информацией. Все эти изменения позволили перейти на абсолютно новый уровень обработки информации, но при этом и возможности злоумышленников существенно возросли. Информация во всех ее формах и видах стала доступна на цифровых носителях и в интернете, в результате проблема ее защиты стала одной из значимых.

За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения информационной безопасности; практически закончено формирование базы правового обеспечения информационной безопасности; приняты федеральные законы: «О государственной тайне», «Об информации, информационных технологиях и о защите информации», «О персональных данных», Гражданский кодекс (ч. 4) и ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Реализованы мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от форм собственности. Развернута работа по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственные системы защиты информации, защиты государственной тайны, лицензирования деятельности в области защиты государственной тайны и сертификации средств защиты информации.

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и методических документов их применения по вопросам обеспечения информационной безопасности Российской Федерации.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;

- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;

- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;

- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих принципах:

- соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;

- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Попытка получить несанкционированный доступ к компьютерной системе или вычислительной сети с целью ознакомиться с ними, выполнить, уничтожить, изменить или похитить программу, или иную информацию квалифицируется как компьютерное пиратство. Компьютерное пиратство – это нарушение авторских прав, т. е. это правонарушение, суть которого – использование произведений науки, литературы и искусства, охраняемых авторским правом, без разрешения авторов или правообладателей или с нарушением условий договора об использовании таких произведений.

К нарушениям авторских прав относят: незаконное копирование и распространение произведения, плагиат, подделка оригинальных произведений искусства с изготовлением копий; нарушение личных прав автора – несогласованное изменение произведения, смена наименования без разрешения и т. д. Как явление, подобные действия прослеживаются в последние 10 лет, но при этом наблюдается тенденция к их стремительному росту по мере увеличения числа смартфонов, планшетов и т. д.

Растет число серьезных нарушений, связанных с умышленными действиями. Так, например, известны случаи внедрения в военные системы; нарушения телевизионной спутниковой связи; вывода из строя электронных узлов регистрации на бензоколонках,

использующих высокочастотные усилители; известны попытки перевода в Швейцарию евробондов на сумму 8,5 млн долл. и разрушения европейской коммуникационной сети связи. Из этого следует, что не только компьютеры, но и другие электронные системы являются объектами злоумышленных действий.

С одной стороны, усложнение аппаратуры и программного обеспечения позволяют снизить вероятность подобных нарушений, с другой, сложность оборудования затрудняет обнаружение, расследование и сбор улик в случае судебного разбирательства. Так, например, немногие обладают необходимыми способностями и техническими знаниями, чтобы обнаружить следы умышленного перепрограммирования или замены чипа.

В настоящее время перед правоохранительными органами при расследовании компьютерных преступлений возникают проблемы, характеризующие одновременно и специфику этого процесса, а именно:

1) сложность в установлении факта совершения компьютерного преступления и решении вопроса о возбуждении уголовного дела;

2) сложность в подготовке и проведении отдельных следственных действий;

3) особенности выбора и назначения необходимых судебных экспертиз;

4) целесообразность использования средств компьютерной техники в расследовании преступлений данной категории;

5) отсутствие методики расследования компьютерных преступлений.

По оценкам отечественных и зарубежных исследователей, решение проблем раскрытия и расследования преступлений данного вида представляет собой задачу на несколько порядков более сложную, чем задачи, сопряженные с их предупреждением. Поэтому уровень латентности компьютерных преступлений определяется в настоящее время в 90 %, а из оставшихся 10 % выявленных раскрывается только 1 %.

Современные условия требуют и определяют необходимость комплексного подхода к формированию законодательства по защите информации, его состава и содержания, соотнесения его со всей системой законов и правовых актов РФ.

Существует следующая структура правовых актов, ориентированных на правовую защиту информации:

1. Международные акты информационного законодательства.

2. Информационно-правовые нормы Конституции Российской Федерации (ст. 2, 23, 24, 29, 33, 41, 42, 44).

3. Отрасли законодательства, акты которых целиком посвящены вопросам информационного законодательства.

4. Отрасли законодательства, акты которых включают отдельные информационно-правовые нормы.

Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации»

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019) *(далее* – Закон № 149-ФЗ) регулирует отношения, возникающие:

- при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;
- создании и использовании информационных технологий и средств их обеспечения;
- защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

2. Закон № 149-ФЗ не затрагивает отношений, регулируемых разделом VII «Права на результаты интеллектуальной деятельности и средства индивидуализации» части 4 Гражданского кодекса Российской Федерации.

Термины и определения, используемые в Законе № 149-ФЗ:

- *информация* – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- *информатизация* – организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов;
- *документированная информация (документ)* – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

- *информационные процессы* – процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

- *информационная система* – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

- *информационные ресурсы* – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

- *информация о гражданах (персональные данные)* – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

- *конфиденциальная информация* – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

- *средства обеспечения автоматизированных информационных систем и их технологий* – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию;

- *собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения* – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;

- *владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения* – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных Законом;

- *пользователь (потребитель) информации* – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Обязанности государства в сфере формирования информационных ресурсов и информатизации:

1. Государственная политика в сфере формирования информационных ресурсов и информатизации направлена на создание условий для эффективного и качественного информационного обеспечения решения стратегических и оперативных задач социального и экономического развития Российской Федерации.

2. Основными направлениями государственной политики в сфере информатизации являются:

- обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;

- формирование и защита государственных информационных ресурсов;

- создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве Российской Федерации;

- создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;

- обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;

- содействие формированию рынка информационных ресурсов, услуг, информационных систем, технологий, средств их обеспечения;

- формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;

- поддержка проектов и программ информатизации;

- создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации;

- развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

Документирование информации является обязательным условием включения информации в информационные ресурсы. Документирование информации осуществляется в порядке, устанавлива-

емом органами государственной власти, ответственными за организацию делопроизводства, стандартизацию документов и их массивов, безопасность Российской Федерации.

Документ, полученный из автоматизированной информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством Российской Федерации.

Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Информационные ресурсы как элемент состава имущества и объект права собственности:

1. Информационные ресурсы могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Отношения, связанные с правом собственности на информационные ресурсы, регулируются гражданским законодательством Российской Федерации.

2. Физические и юридические лица являются собственниками тех документов, массивов документов, которые созданы за счет их средств, приобретены ими на законных основаниях, получены в порядке дарения или наследования.

3. Российская Федерация и субъекты Российской Федерации являются собственниками информационных ресурсов, создаваемых, приобретаемых, накапливаемых за счет средств федерального бюджета, бюджетов субъектов Российской Федерации, а также полученных путем иных установленных законом способов.

Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне. Собственник информацион-

ных ресурсов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти.

Информационные ресурсы, являющиеся собственностью организаций, включаются в состав их имущества в соответствии с гражданским законодательством Российской Федерации.

Информационные ресурсы, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите в составе государственного имущества.

Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации. Собственник информационных ресурсов пользуется всеми правами, предусмотренными законодательством Российской Федерации, в том числе он имеет право:

- назначать лицо, осуществляющее хозяйственное ведение информационными ресурсами или оперативное управление ими;
- устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;
- определять условия распоряжения документами при их копировании и распространении.

Право собственности на средства обработки информации не создает права собственности на информационные ресурсы, принадлежащие другим собственникам. Документы, обрабатываемые в порядке предоставления услуг или при совместном использовании этих средств обработки, принадлежат их владельцу. Принадлежность и режим производной продукции, создаваемой в этом случае, регулируются договором.

Государственные информационные системы:

1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

2. Государственные информационные системы создаются, модернизируются и эксплуатируются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд либо законодательством Российской Федерации о государственно-частном партнерстве,

о муниципально-частном партнерстве, законодательством о концессионных соглашениях, а в случаях, если эксплуатация государственных информационных систем осуществляется без привлечения средств бюджетной системы Российской Федерации, в соответствии с иными федеральными законами.

3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления – Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами. В случае, если при создании или эксплуатации государственных информационных систем предполагается осуществление или осуществляется обработка общедоступной информации, предусмотренной перечнями, утверждаемыми в соответствии со ст. 14 Федерального закона от 9 февраля 2009 года № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», государственные информационные системы должны обеспечивать размещение такой информации в интернете в форме открытых данных.

Формирование государственных информационных систем в соответствии со ст. 13 Закона № 149-ФЗ осуществляется гражданами, органами государственной власти, органами местного самоуправления, организациями и общественными объединениями.

При регистрации юридических лиц регистрационные органы обеспечивают их перечнями представляемых в обязательном порядке документов и адресами их представления. Перечень представляемой в обязательном порядке документированной информации прилагается к уставу каждого юридического лица (положению о нем). Необеспечение регистрационными органами регистрируемых юридических лиц перечнем представляемых в обязательном порядке документов с адресами их представления не является основанием для отказа в регистрации. Должностные лица регистрационных органов, виновные в необеспечении регистрируемых юридических лиц перечнями представляемых в обязательном порядке документов

с адресами их представления привлекаются к дисциплинарной ответственности вплоть до снятия с должности.

Информационные ресурсы по категориям доступа:

1. Государственные информационные ресурсы Российской Федерации являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.

2. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

3. Запрещено относить к информации с ограниченным доступом:

- законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

- документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

- документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;

- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации «О государственной тайне».

Отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федера-

ции, за исключением случаев, предусмотренных ст. 9 Закона № 149-ФЗ и Законом № 152-ФЗ.

Информация о гражданах (персональные данные):

1. Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых негосударственными организациями, должны быть закреплены на уровне федерального закона. Персональные данные относятся к категории конфиденциальной информации. Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

2. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

4. Подлежит обязательному лицензированию деятельность негосударственных организаций и частных лиц, связанная с обработкой и предоставлением пользователям персональных данных. Порядок лицензирования определяется законодательством Российской Федерации.

5. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании Федеральных законов № 149-ФЗ и № 152-ФЗ.

Целями защиты информации и прав субъектов в области информационных процессов и информатизации являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества, государства;

- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Основные положения Федерального закона «О персональных данных»

Федеральный закон от 27.07.06 № 152-ФЗ «О персональных данных» *(далее* – Закон № 152-ФЗ) регулирует отношения по обработке информации, относящейся к физическим лицам (субъектам персональных данных), в государственных и муниципальных органах юридическими и физическими лицами (операторами).

В соответствии с законом № 152-ФЗ:

- *персональные данные (далее* – ПД*)* – любая информация о физическом лице (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация);

- *оператор* – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осу-

ществляющие обработку ПД, а также определяющие цели и содержание обработки ПД;

- *обработка персональных данных* – действия (операции) с ПД, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПД.

В следующих случаях не требуется согласия на обработку ПД субъекта ПД:

1) обработка ПД осуществляется на основании федерального закона, устанавливающего ее цель, условия получения ПД и круг субъектов, ПД которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка ПД осуществляется в целях исполнения договора, одной из сторон которого является субъект ПД;

3) обработка ПД осуществляется для статистических или иных научных целей при условии обязательного обезличивания ПД;

4) обработка ПД необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПД, если получение согласия субъекта ПД невозможно;

5) обработка ПД необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка ПД осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта ПД;

7) осуществляется обработка ПД, подлежащих опубликованию в соответствии с федеральными законами, в том числе ПД лиц, замещающих государственные должности, должности государственной гражданской службы, ПД кандидатов на выборные государственные или муниципальные должности.

На обработку своих ПД субъект должен дать согласие, причем он имеет право его отозвать в любой момент. Согласие может быть выражено в устной или письменной форме – в зависимости от категории ПД, а также характера их обработки. Согласие субъекта ПД в письменной форме требуется в следующих случаях:

- при обработке специальных категорий ПД, касающихся расовой, национальной принадлежности, политических взглядов, ре-

лигиозных или философских убеждений, состояния здоровья, интимной жизни. Обрабатывать такие сведения без письменного согласия субъекта категорически запрещено (за исключением случаев, когда они являются общедоступными). Письменное согласие на подобные действия необходимо, даже если субъекта ПД и оператора связывают договорные отношения. В общественных объединениях или религиозных организациях обработка специальных категорий ПД членов (участников) осуществляется при условии, что ПД не будут распространяться без согласия субъектов, данного в письменной форме;

- при обработке биометрических ПД – сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (сведения об особенностях строения папиллярных узоров пальцев рук человека, сетчатки глаз, о коде ДНК и т. д.). Это требование также должно соблюдаться независимо от наличия договорных отношений между субъектом ПД и оператором, кроме отношений, связанных с прохождением государственной гражданской службы;

- при передаче ПД субъекта оператором через государственную границу РФ органу власти иностранного государства, физическому или юридическому лицу иностранного государства, не обеспечивающему адекватную защиту прав субъекта ПД.

В соответствии с Законом № 152-ФЗ письменное согласие субъекта на обработку его персональных данных должно включать:

- фамилию, имя, отчество, адрес субъекта ПД, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование (фамилия, имя, отчество) и адрес оператора, получающего согласие субъекта ПД;

- цель обработки ПД;

- перечень ПД, на обработку которых дается согласие субъекта ПД;

- перечень действий с ПД, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПД;

- срок, в течение которого действует согласие, а также порядок его отзыва.

Независимо от того, в письменной или устной форме получено согласие субъекта на обработку его ПД, на оператора возлагается обязанность по доказыванию факта получения такого согласия.

Оператор обязан предоставить субъекту ПД доступ к его данным в любой момент по его просьбе. У субъекта есть право на получение следующей информации:

1) подтверждение факта обработки ПД оператором, а также цель такой обработки;

2) способы обработки ПД, применяемые оператором;

3) сведения о лицах, которые имеют доступ к ПД или которым может быть предоставлен такой доступ;

4) перечень обрабатываемых ПД и источник их получения;

5) сроки обработки ПД, в том числе сроки их хранения;

6) сведения о том, какие юридические последствия для субъекта ПД может повлечь за собой обработка его данных.

Права на результаты интеллектуальной деятельности и средства индивидуализации

В настоящий момент основным нормативным актом, регламентирующим использование и защиту авторских прав на программное обеспечение, является Гражданский кодекс Российской Федерации *(далее* – ГК РФ*)*. Права на результаты интеллектуальной деятельности и средства индивидуализации описаны в Гражданском кодексе в разделе VII части 4-й, главы которой следует рассматривать взаимосвязано, так как их положения непосредственно затрагивают правовую охрану программ для ЭВМ.

В соответствии с действующим законодательством Российской Федерации, за нарушение авторских прав предусмотрено наступление гражданской, уголовной и административной ответственности.

В соответствии с гл. 70 ГК РФ, автор программы и иные правообладатели вправе требовать:

- признания прав;

- восстановления положения, существовавшего до нарушения права, и прекращения действий, нарушающих право или создающих угрозу его нарушения;

- возмещения причиненных убытков, в размер которых включается сумма доходов, неправомерно полученных нарушителем. ГК РФ определяет, что под убытками понимают: а) расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права; б) утрату или повреждение его имущества (реальный ущерб); в) неполученные доходы, которые

это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода). Если лицо, нарушившее право, получило вследствие этого доходы, лицо, право которого нарушено, вправе требовать возмещения наряду с другими убытками упущенной выгоды в размере не меньшем, чем такие доходы;

- принятия иных, предусмотренных законодательными актами мер, связанных с защитой их прав (их неполный перечень дается в ст. 12 ГК РФ).

Весьма серьезная ответственность установлена за нарушение авторских прав Уголовным кодексом Российской Федерации *(далее* – УК РФ*)*. Так, в соответствии со ст. 146 УК РФ (нарушение авторских и смежных прав): «Незаконное использование объектов авторского права или смежных прав, а равно присвоение авторства, если эти деяния причинили крупный ущерб наказываются штрафом в размере от двухсот до четырехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода, осужденного за период от двух до четырех месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, наказываются штрафом в размере от четырехсот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода, осужденного за период от четырех до восьми месяцев, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до пяти лет».

Как видно, уголовная ответственность наступает при наличии «крупного ущерба», его критериями являются: размер причиненного ущерба, количество потерпевших, степень нарушения прав гражданина, тяжесть причиненного морального вреда. В судебной практике крупным ущербом признается ущерб, превышающий десятикратный минимальный размер оплаты труда.

При нарушении авторских прав могут быть совершены преступления, указанные и в иных статьях УК РФ, например:

- ст. 272 Неправомерный доступ к компьютерной информации;

- ст. 273 Создание, использование и распространение вредоносных программ для ЭВМ;

- ст. 274 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

На основании вышеизложенного можно сделать вывод, что законодательная база достаточно разработана, чтобы уже сейчас эффективно выявлять и наказывать преступников – нарушителей авторских прав.

Очевидно, что для наиболее эффективной работы в этой области необходимо сотрудничество производителей программных продуктов и правоохранительных органов. Представляется необходимым создание технически и юридически грамотных союзов и ассоциаций для целенаправленной борьбы с «пиратством» и обеспечения представления интересов производителей во всех ветвях власти, в том числе и на законодательном уровне, для разработки и совершенствования правовой базы борьбы с преступностью в области авторского права.

Промышленный шпионаж (также экономический или корпоративный шпионаж) – форма недобросовестной конкуренции, при которой осуществляется незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну с целью получения преимуществ при осуществлении предпринимательской деятельности, а равно получения материальной выгоды.

Основное предназначение промышленного шпионажа – экономия средств и времени, которые требуется затратить, чтобы догнать конкурента, занимающего лидирующее положение, либо не допустить в будущем отставания от конкурента, если тот разработал или разрабатывает новую перспективную технологию, а также чтобы выйти на новые для предприятия рынки.

Это справедливо и в отношении межгосударственной конкуренции, где к вопросам экономической конкурентоспособности добавляются и вопросы национальной безопасности.

Основное отличие промышленного шпионажа от конкурентной разведки в том, что промышленный шпионаж нарушает нормы законодательства, прежде всего, уголовного. Промышленный шпионаж остается и будет оставаться мощным инструментом государственных разведок, предназначение которых – прямое нарушение законов иностранных государств в интересах и по поручению своей страны.

На уровне предприятий в последнее время все чаще делается выбор в пользу конкурентной разведки, так как предприятие не имеет

полномочий государственных разведок, поэтому в случае провала операции промышленного шпионажа рискует быть привлеченным к уголовной ответственности, а также понести репутационные риски.

По мнению ряда исследователей, во многих случаях предприятия малого и среднего бизнеса к промышленному шпионажу прибегают потому, что не обучены методам конкурентной разведки, а зачастую и вообще не знают об их существовании. В ситуации, когда необходимость выживания или повышения конкурентоспособности существует объективно, а о наличии законных методов достижения результата предприятие не информировано, часть компаний встает на путь промышленного шпионажа. В связи с этим, общества профессионалов конкурентной разведки всего мира включают в свои задачи просветительские функции.

К методам промышленного шпионажа относятся:

- подкуп лиц, имеющих доступ к информации, относящейся к коммерческой, служебной, или иной охраняемой законом тайне;

- шантаж в отношении того же круга лиц;

- кража носителей с информацией, представляющей коммерческую, служебную или иную охраняемую законом тайну;

- внедрение агента на предприятие или в страну конкурента с заданием получить доступ к информации или продукции, которые составляют предмет коммерческой или иной охраняемой законом тайны;

- незаконный доступ к коммерчески значимой информации с помощью использования технических средств (прослушивание телефонных линий, незаконное проникновение в компьютерные сети и т. п.).

КРИПТОГРАФИЯ. КЛАССИФИКАЦИЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

Существует два основных способа защиты секретов. Во-первых, можно попытаться скрыть сам факт существования секрета: нет секрета – нет и желающих его узнать. Основной прием, используемый для достижения этой цели, – стеганография, то есть передача тайной информации под видом общедоступной. Прежде для этих целей использовались тексты (письма, книги, газетные статьи), определенные буквы или слова которых и составляли текст секретного послания. Теперь, в условиях всеобщей компьютеризации, наиболее распространенный стеганографический материал – это

графические, звуковые и другие мультимедийные данные, формат которых позволяет замещать наименее значимую часть исходной информации на любую произвольную (собственно, на тот самый секрет, который требуется спрятать). При этом главное правило формулируется так: все произведенные преобразования не должны быть заметны невооруженным глазом или ухом.

Второй способ основан на прямо противоположном принципе: мы ни от кого не скрываем, что передаем или храним важную секретную информацию и не предпринимаем никаких действий для предотвращения доступа к ней посторонних лиц, но информация при этом передается или хранится в таком виде, что понять ее истинный смысл могут только посвященные. Сделать это позволяет криптография. Секретные данные шифруются с помощью определенного алгоритма, чтобы прочитать их сначала потребуется их расшифровать. Избирательность доступа к информации обеспечивается тем, что шифрование и расшифровка производятся с использованием некой ключевой информации, которой обладают только те, кому разрешен доступ к секретным данным.

Наука, занимающаяся вопросами безопасной связи, т. е. посредством зашифрованных сообщений называется *криптологией*. Она в свою очередь разделяется на два направления – *криптографию* и *криптоанализ*.

Криптография – наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров. Она занимается поиском математических методов преобразования информации.

Криптографическая система – семейство преобразований шифра и совокупность ключей (т. е. алгоритм + ключи). Само по себе описание алгоритма не является криптосистемой, только дополненное схемами распределения и управления ключами оно становится системой.

Криптосистемы могут обеспечивать не только секретность передаваемых сообщений, но и их аутентичность (подлинность), а также подтверждение подлинности пользователя.

Одно из основных правил криптографии (если рассматривать ее коммерческое применение, так как на государственном уровне все несколько иначе) можно выразить следующим образом: взлом шифра с целью прочесть закрытую информацию должен обойтись злоумышленнику гораздо дороже, чем эта информация стоит на самом деле.

Шифр – совокупность обратимых преобразований множества открытых текстов (т. е. исходного сообщения) на множество зашифрованных текстов, проводимых с целью их защиты. Конкретный вид преобразования определяется с помощью ключа шифрования.

Зашифрование – процесс применения шифра к открытому тексту.

Расшифрование – процесс обратного применения шифра к зашифрованному тексту.

Дешифрование – попытка прочесть зашифрованный текст без знания ключа, т. е. взлом шифротекста или шифра.

Здесь следует подчеркнуть разницу между расшифрованием и дешифрованием. Первое действие проводится законным пользователем, знающим ключ, а второе – криптоаналитиком или мощным хакером, не знающим ключ.

Гаммирование – процесс наложения по определенному закону гаммы шифра на открытые данные.

Под гаммой шифра понимается псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для шифрования открытых данных и расшифровывания зашифрованных данных.

Имитозащита – это защита системы шифрованной связи от навязывания ложных данных.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

- достаточная криптостойкость (надежность закрытия данных);
- простота процедур шифрования и расшифрования;
- незначительная избыточность информации за счет шифрования;
- нечувствительность к небольшим ошибкам шифрования и др.

Все криптографические алгоритмы обычно разделяют на *симметричные* и *асимметричные*.

Симметричные алгоритмы предполагают, что данные будут зашифровываться и расшифровываться на одних и тех же ключах, то есть и передающая, и принимающая стороны обладают одинаковой ключевой информацией.

Доставить эту информацию абонентам нужно тайно, и сделать это можно двумя способами:

1. Ключи доставляются физически (в виде электронных ключей, пластиковых карточек, паролей, которые администратор сообщает лично, и т. п.);

2. Ключи передаются по каналу связи в зашифрованном виде (предполагается, что до этого абоненты уже располагали некой ключевой информацией).

Асимметричные алгоритмы (алгоритмы с открытым ключом) появились сравнительно недавно и произвели настоящую революцию в криптографии, такой алгоритм состоит из двух частей ключа: для шифрования и для расшифровки. При этом, зная ключ шифрования, практически невозможно вычислить ключ расшифровки.

Классификация криптографических систем. Все традиционные криптографические системы подразделяются по видам шифров.

1. Шифры перестановки:
- шифр перестановки «скитала» (цилиндр + намотанная кожа);
- шифрующие таблицы (запись букв алфавита в матрицу);
- применение магических квадратов.

2. Шифры простой замены:
- полибианский квадрат;
- система шифрования Цезаря (сдвиг текста на определенное число позиций);
- аффинная система подстановок Цезаря;
- система Цезаря с ключевым словом;
- шифрующие таблицы Трисемуса;
- биграммный шифр Плейфейра;
- криптосистема Хилла;
- система омофонов.

3. Шифры сложной замены:
- шифр Гронсфельда.
- система шифрования Вижинера;
- шифр «двойной квадрат» Уитстона;
- одноразовая система шифрования;
- шифрование методом Вернама;
- роторные машины.

4. Шифрование методом гаммирования.

5. Шифрование, основанное на аналитических преобразованиях шифруемых данных.

Стандартизация в криптографии. Все технологии, применяемые в информационно-вычислительных системах, регулируются множеством стандартов и соглашений, выработанных компаниями,

группами компаний или независимыми организациями. Не стала исключением и криптография.

Пожалуй, первым стандартизованным криптографическим алгоритмом стал DES – национальный стандарт шифрования коммерческой информации в США, разработанный фирмой IBM и принятый еще в 1977 г. DES – симметричный блочный алгоритм с секретным ключом длиной 56 бит. В качестве официального стандарта этот шифр прослужил Соединенным Штатам вплоть до 2000 г., пережив за это время периоды популярности и яростной критики. Алгоритм DES был включен в состав многих коммерческих программных продуктов, получил распространение по всему миру и лег в основу большей части последующих разработок в области блочных шифров.

Главным объектом нападок стала недостаточная надежность шифрования DES: за 25 лет существования стандарта вычислительные средства совершили огромный скачок в развитии, сделав возможным вскрытие этого шифра, что неоднократно было доказано на практике. Пытаясь повысить стойкость алгоритма без существенной его переработки, криптографы предложили новую его версию – Triple DES (3DES). В этой криптосхеме предусматривается трехкратное применение DES с разными ключами, в результате чего длина ключа увеличивается до 168 бит, что существенно повышает надежность шифрования. Именно этот алгоритм нередко применяется в новых версиях программ, использовавших ранее обычный DES.

В 2000 г. в США был объявлен конкурс на лучший криптоалгоритм, победитель которого должен был стать новым стандартом страны на коммерческое шифрование – AES. Этот стандарт призван сменить устаревший DES и стать, как гласит рекламный слоган, стандартом шифрования XXI века, и это утверждение, учитывая 25-летнюю историю DES, не является просто громкой фразой. Пройдя многоуровневый отбор и преодолев жесточайшую конкуренцию со стороны американских информационных гигантов, победителем в конкурсе стал шифр, разработанный европейскими криптографами, – Rijndael.

Отечественным аналогом DES является ГОСТ 28147-89. Этот шифр был разработан в 70-х годах прошлого века в КГБ СССР и имел гриф «совершенно секретно». С течением времени гриф снижался, и в 1989 г. этот алгоритм стал применяться «для служебного

пользования»; этот гриф, как известно, не является секретным, что дало возможность провести шифр через процедуру стандартизации. В начале 90-х годов гриф был окончательно снят, а сам алгоритм признан уже не советским, а российским стандартом.

Преимущества перед DES наш алгоритм имел существенные.

Во-первых, в ГОСТ используются ключи длиной 128 бит, что позволяет ему до сих пор оставаться достаточно надежным для коммерческого использования.

Во-вторых, этот алгоритм создавался с расчетом на то, чтобы в равной степени эффективно реализовываться как аппаратными, так и программными средствами. Это позволило при большей надежности иметь и серьезное преимущество перед американским стандартом в скорости работы. Все эти плюсы стали залогом долголетия отечественного алгоритма и позволили ему пережить заморский аналог.

Наиболее распространенным в мире симметричным поточным шифром является RC4. Он был разработан в 1989 г. и запатентован; его алгоритм был объявлен коммерческой тайной и передавался под подписку о неразглашении после приобретения лицензии. Этот шифр включили в состав своих программных продуктов многие крупные софтверные компании. В 1996 г. криптосхема шифра RC4 была анонимно опубликована в интернете, после чего стала активно исследоваться на предмет слабостей и возможных подходов к вскрытию, но с тех пор не было найдено ни одного серьезного просчета разработчиков, который бы позволил при корректной реализации алгоритма эффективно его взламывать.

Одним из первых алгоритмов шифрования с открытым ключом стал шифр RSA. Этот алгоритм оказался настолько гибким и эффективным, что стал де-факто стандартом в асимметричной криптографии. Именно этот шифр используется практически во всех программах, где нужно применить алгоритм с открытым ключом. Стойкость шифра зависит от длины ключа, но, если, пожертвовав скоростью, применить ключевую последовательность достаточного размера, можно добиться любой требуемой надежности

.

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Целью практических работ является изучение алгоритмов, применяемых для защиты информации в компьютерных системах и сетях.

Задание № 1
Алгоритм шифрования

Цель работы: проанализировать существующие простейшие алгоритмы шифрования.

Задания:

1. Разработать собственный алгоритм шифрования.
2. Разработать форму, содержащую: 3 текстовых поля, кнопку «Шифровать», кнопку «Расшифровать».
3. Реализовать разработанный алгоритм на любом языке программирования.

Методика выполнения практической работы. Ознакомиться с существующими простыми алгоритмами шифрования. В результате изучения алгоритмов и анализа литературы сформировать принципы работы алгоритмов шифрования.

Требования к работе:

- программа шифрования должна быть наделена понятным и удобным пользовательским интерфейсом;
- алгоритм шифрования в обязательном порядке должен использовать математические и/или побитовые функции;
- разработанный алгоритм должен приводить к полной утрате всех статистических закономерностей исходного сообщения.

Основные теоретические положения. Все существующие криптографические методы сводятся к следующим классам преобразований:

1. *Многоалфавитная подстановка* – наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.
2. *Перестановки* – несложный метод криптографического преобразования. Используется, как правило, в сочетании с другими методами.

3. *Гаммирование* – этот метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

4. *Блочные шифры* – представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста.

В качестве примера одного из классов преобразований можно привести алгоритм Цезаря (табл.1). Он относится к первой группе.

Подмножество $C_m = \{C_k: 0 \le k < m\}$ симметрической группы $SYM(Z_m)$, содержащее m подстановок $C_k: j \to (j + k) \pmod m$, $0 \le k < m$, называется подстановкой Цезаря.

Умножение коммутативно, $C_kC_j = C_jC_k = C_{j+k}$, C_0 – идентичная подстановка, а обратной к $C_к$ является $C_k^{-1} = C_{m-k}$, где $0 < k < m$. Семейство подстановок Цезаря названо по имени римского императора Гая Юлия Цезаря, который поручал Марку Туллию Цицерону составлять послания с использованием 50-буквенного алфавита и подстановки C_3.

Подстановка определяется по таблице замещения, содержащей пары соответствующих букв «исходный текст – шифрованный текст». Для C_3 подстановки приведены в табл. 1. Стрелка (→) означает, что буква исходного текста (слева) шифруется при помощи C_3 в букву шифрованного текста (справа).

Системой Цезаря называется моноалфавитная подстановка, преобразующая n-грамму исходного текста $(x_0, x_1, ..., x_{n-1})$ в n-грамму шифрованного текста $(y_0, y_1, ..., y_{n-1})$ в соответствии с правилом:

$$y_i = C_k(x_i),\ 0 \le i < n.$$

Например, словосочетание «алгоритм шифрования» посредством подстановки C_3 преобразуется в «гожсулхпвылчусегрлб».

При своей несложности система легкоуязвима. Если злоумышленник имеет шифрованный и соответствующий исходный текст или шифрованный текст выбранного злоумышленником исходного текста, то определение ключа и дешифрование исходного текста тривиальны.

Более эффективны обобщения подстановки Цезаря – *шифр Хилла* и *шифр Плэйфера*. Они основаны на подстановке не отдельных символов, а 2-грамм (шифр Плэйфера) или n-грамм (шифр Хилла). При более высокой криптостойкости они значительно сложнее для реализации и требуют достаточно большого количества ключевой информации.

Таблица 1

Система подстановки Цезаря

А→г	Й→м	Т→х	Ы→ю
Б→д	К→н	У→ц	Ь→я
В→е	Л→о	Ф→ч	Э→_
Г→ж	М→п	Х→ш	Ю→а
Д→з	Н→р	Ц→щ	Я→б
Е→и	О→с	Ч→ъ	_→в
Ж→й	П→т	Ш→ы	
З→к	Р→у	Щ→ь	
И→л	С→ф	Ъ→э	

Задание № 2
Алгоритм шифрования с ключом

Цель работы: проанализировать существующие простейшие алгоритмы шифрования с ключом.

Задания:

1. Разработать собственный алгоритм шифрования и дешифрования данных с ключом.
2. Разработать форму содержащую: 3 текстовых поля, кнопку «Шифровать», кнопку «Расшифровать», текстовое поле «Ключ» для шифрации, текстовое поле «Ключ» для дешифрации.
3. Реализовать разработанный алгоритм на любом языке программирования.

Методика выполнения практической работы. Ознакомиться с существующими простыми алгоритмами шифрования с ключом. В результате изучения и анализа литературы сформировать принципы работы алгоритмов шифрования.

Требования к работе:

- программа шифрования должна быть наделена понятным и удобным пользовательским интерфейсом;
- алгоритм шифрования в обязательном порядке должен использовать математические и/или побитовые функции;
- разработанный алгоритм должен приводить к полной утрате всех статистических закономерностей исходного сообщения;
- максимально возможная длина ключа шифрования – 100 символов, минимальная длина ключа – 1 символ.

Основные теоретические положения. Все криптоалгоритмы с ключом делятся на симметричные и асимметричные. В симметричных криптоалгоритмах ключи, используемые на передающей и принимающей сторонах, полностью идентичны. Такой ключ несет в себе всю информацию о засекречивании сообщения и поэтому не должен быть известен никому, кроме двух участвующих в разговоре сторон. Поэтому в отношении ключа симметричных систем часто применяется термин секретный ключ, а сами подобные системы называются шифрами на секретном ключе.

Симметричное шифрование можно применять как при отправке сообщений между двумя пользователями, разделенными большим расстоянием, так и при отправке «посланий» одним и тем же человеком самому себе, но во времени. Примером подобных отправлений является шифр файлов на жестких дисках и сменных носителях с тем, чтобы другие пользователи тех же ЭВМ не могли считать информацию в отсутствие владельца.

В асимметричном шифровании для шифрования сообщения применяется один ключ, а для дешифрования другой. На рис. 1 показана схема передачи информации абонентом А абоненту В.

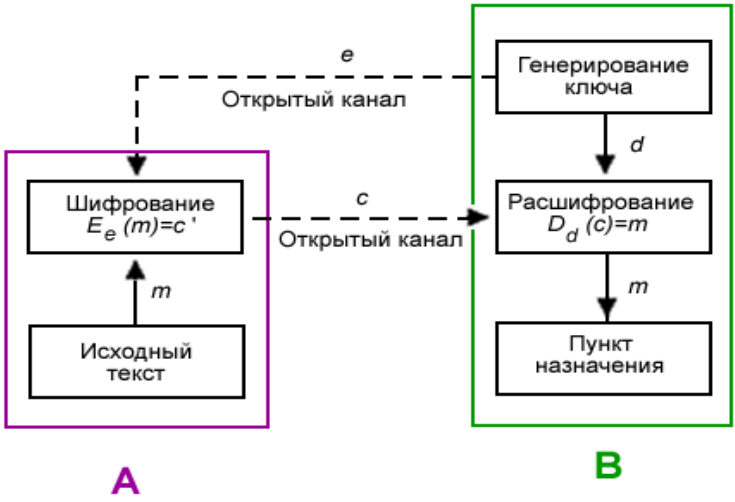

Рис. 1. Шифрование с открытым ключом

1. Абонент B выбирает пару (*e*, *d*) и шлет ключ шифрования *e* (открытый ключ) абоненту A по открытому каналу, а ключ расшифрования *d* (закрытый ключ) защищен и секретен (он не должен передаваться по открытому каналу, либо его подлинность должна быть гарантирована некоторым сертифицирующим органом).

2. Чтобы послать сообщение *m* абоненту B, абонент A применяет функцию шифрования, определенную открытым ключом *e:*

$$E_e(m) = c,$$

где *c* – полученный шифротекст.

3. Абонент B расшифровывает шифротекст *c*, применяя обратное преобразование D_d, однозначно определенное значением *d*.

Задание № 3
Симметричный алгоритм шифрования

Цель работы: исследование структуры симметричных алгоритмов шифрования: AES, ГОСТ 28147-89, DES, RC6, IDEA, SEED.

Задания:

1. Реализовать один из существующих симметричных алгоритмов шифрования: AES, ГОСТ 28147-89, DES, RC6, IDEA, SEED.
2. Разработать форму, содержащую: 3 текстовых поля, кнопку «шифровать», кнопку «расшифровать», текстовое поле ключ для шифрации, текстовое поле ключ для дешифрации.
3. Организовать дополнительный интерфейс настройки алгоритма по необходимости.
4. Реализовать разработанный алгоритм на любом языке программирования.

Методика выполнения практической работы. Изучить один из алгоритмов работы симметричного шифрования и реализовать на каком-либо языке программирования.

Требования к работе:

- программа шифрования должна быть наделена понятным и удобным пользовательским интерфейсом;
- полная реализация выбранного алгоритма;
- запрещено использование любых сторонних библиотек.

Основные теоретические положения. Симметричные криптосистемы – способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования един-

ственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в секрете обеими сторонами и выбирается ими до начала обмена сообщениями. Симметричные шифры могут быть блочными:

1. Блочные шифры обрабатывают информацию блоками определенной длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является лавинный эффект – нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.

2. В поточных шифрах шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования. Поточный шифр может быть легко создан на основе блочного (например, ГОСТ 28147-89 в режиме гаммирования), запущенного в специальном режиме.

Основными параметрами алгоритмов симметричного шифрования являются:

- стойкость;
- длина ключа;
- число раундов;
- длина обрабатываемого блока;
- сложность аппаратной/программной реализации;
- сложность преобразования.

В качестве примера алгоритма симметричного шифрования можно рассмотреть отечественный алгоритм шифрования ГОСТ 28147-89, который определен в стандарте. Алгоритм шифрует данные 64-битными блоками с использованием 256-битного ключа шифрования. Базовым режимом шифрования по ГОСТ 28147-89 является режим простой замены. Для зашифрования в этом режиме открытый текст сначала разбивается на две половины (младшие биты – A, старшие биты – B). На i-ом цикле используется подключ K_i:

$$A_{i+1} = B \oplus f(A_i, K_i),$$

где $\oplus$ = двоичное «исключающее или»)

$$B_{i+1} = A_i.$$

Выполняется 32 раунда преобразований, в каждом из которых предусмотрены следующие операции (рис. 2):

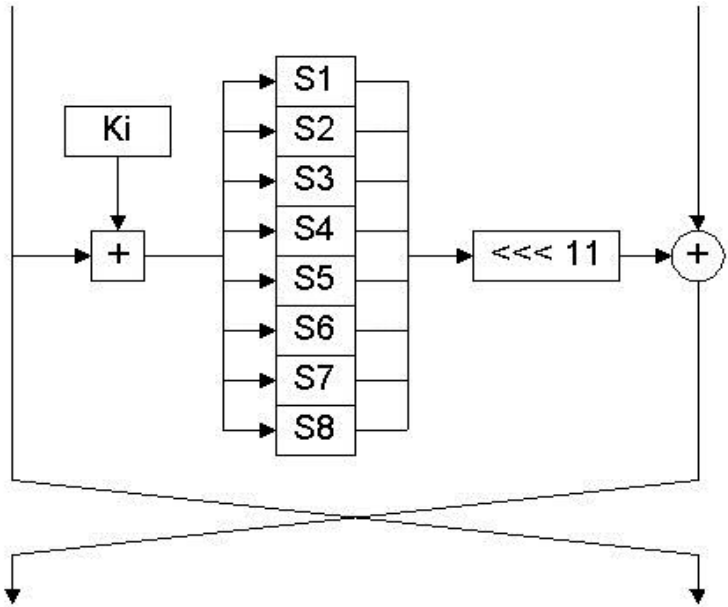

Рис. 2. Раунд алгоритма ГОСТ 28147-89

Шаг 0. Один из 32-битных субблоков данных складывается с 32-битным значением ключа раунда ***Ki*** по модулю 232.

Шаг 1. Результат предыдущей операции разбивается на 8 фрагментов по 4 бита, которые параллельно «прогоняются» через 8 таблиц замен **S1 … S8**. Таблицы замен в стандарте не определены. В качестве примера реализации можно привести следующий исходный код:

```
for (int i = 7; i > -1; i--)
{
S[i] = (byte)((*N1) & 0x0F);
S[i] = H[i,S[i]];
(*N1) = (*N1) >> 4;
}
```

Шаг 2. 4-битные фрагменты (после замен) объединяются обратно в 32-битный субблок, значение которого циклически сдвигается влево на 11 бит.

```
for (int i = 0; i < 8; i++)
{
```

```
(*N1) = (*N1) | S[i];
(*N1) = (*N1) << 4;
}
rot Rot = new rot();
(*N1) = Rot.left((*N1),11);
```

где класс rot описан следующим образом:

```
public class rot
{
    private const uint intSize = sizeof(int);
    public uint left(uint N, int n)
    {
        uint a;
        uint k = (uint)(1 << (int)(intSize - 1));
        for (int i = 1; i <= (n % intSize); i++)
        {
            a = N & k;
            N = N << 1;
            a = (uint)((int)a >> (int)(intSize - 1));
            N = N | a;
        }
        return N;
    }
    public uint right(uint N, int n)
    {
        uint a;
        for (int i = 1; i <= (n % intSize); i++)
        {
            a = N & 1;
            N = N >> 1;
            a = (uint)((int)a << (int)(intSize - 1));
            N = N | a;
        }
        return N;
        }
       }
```

Шаг 3. Обработанный предыдущими операциями субблок накладывается на необработанный с помощью побитовой логической операции «исключающее или» (XOR).

*(*N1) = (*N1) ^ (*N2)*;

Шаг 4. Субблоки меняются местами.

Процедура расширения ключа в алгоритме ГОСТ 28147-89 фактически отсутствует: в раундах шифрования последовательно используются 32-битные фрагменты **K1**… **K8** исходного 256-битного ключа шифрования в следующем порядке: **K1, K2, K3, K4, K5, K6, K7, K8** – за исключением последних 8 раундов – в раундах с 25-го по 31-й фрагменты используются в обратном порядке.

Расшифрование полностью аналогично зашифрованию, но с другим порядком использования фрагментов ключа:

- в прямом порядке – в первых 8 раундах;
- в остальных раундах – в обратном порядке.

Стандарт также предусматривает и описывает различные режимы применения алгоритма:

- описанный выше режим простой замены;
- режимы гаммирования и гаммирования с обратной связью, предусматривающие вычисление с помощью описанных выше преобразований псевдослучайной последовательности – гаммы шифра – и ее наложение на шифруемый текст;
- режим вычисления имитовставки – криптографической контрольной суммы, используемой для подтверждения целостности данных; в данном режиме выполняется 16 раундов преобразований вместо 32.

Как видно из описания, алгоритм ГОСТ 28147-89 является весьма простым в реализации, что является его несомненным достоинством.

К достоинствам ГОСТа можно отнести:

- бесперспективность силовой атаки (XSL-атаки в учет не берутся, так как их эффективность на данный момент полностью не доказана);
- эффективность реализации и соответственно высокое быстродействие на современных компьютерах;
- наличие защиты от навязывания ложных данных (выработка имитовставки) и одинаковый цикл шифрования во всех четырех алгоритмах ГОСТа.

На рис. 3 представлен результат работы алгоритма шифрования ГОСТ 34.10-2001. В левом текстовом поле приведен текст подвергаемый шифрованию. В правом текстовом поле приведен уже зашифрованный текст, отраженный в китайской раскладке.

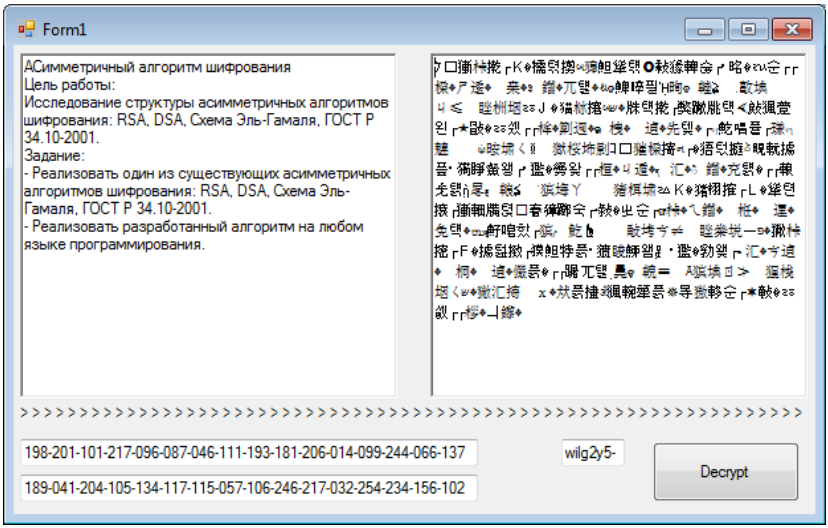

Рис. 3. Форма Алгоритм шифрования ГОСТ 34.10-2001

Задание № 4
Асимметричный алгоритм шифрования

Цель работы: исследование структуры асимметричных алгоритмов шифрования: RSA, DSA, схема Эль-Гамаля, ГОСТ Р 34.10-2001.

Задания:

1. Реализовать один из существующих асимметричных алгоритмов шифрования: RSA, DSA, схема Эль-Гамаля, ГОСТ Р 34.10-2001.

2. Реализовать разработанный алгоритм на любом языке программирования.

Методика выполнения практической работы. Выбрать один из алгоритмов симметричного шифрования, изучить алгоритм его работы и реализовать на каком-либо языке программирования.

Требования к работе:

- программа шифрования должна быть наделена понятным и удобным пользовательским интерфейсом;
- полная реализация выбранного алгоритма;
- запрещено использование любых сторонних библиотек.

Основные теоретические положения. Примером асимметричного алгоритма шифрования может являться схема Эль-Гамаля, которая может быть использована как для формирования цифровых подписей, так и шифрования данных. Безопасность данной схемы обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

В настоящее время наиболее перспективными системами криптографической защиты являются системы с открытым ключом. В таких системах для шифрования сообщения используется закрытый ключ, а для расшифрования – открытый.

Открытый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифровывание данных с помощью открытого ключа невозможно.

Для расшифрования данных получатель зашифрованной информации использует секретный ключ, который не может быть определен из открытого ключа.

При использовании алгоритма шифрования Эль-Гамаля длина шифротекста вдвое больше длины исходного открытого текста ***M***. В реальных схемах шифрования необходимо использовать в качестве модуля n большое простое число, имеющее в двоичном представлении длину 512… 1024 бит.

Следует отметить, что формирование каждой подписи по данному методу требует нового значения ***k***, причем это значение должно выбираться случайным образом. Если нарушитель раскроет значение ***k***, повторно используемое отправителем, то может раскрыть и секретный ключ ***x*** отправителя. Ниже приведен алгоритм шифрования данных по схеме Эль-Гамаля.

Шаг 1. Определение открытого *y* и секретного *x* ключей.

Шаг 1.1. Выбор значения секретного ключа *x*, $x < p$.

Шаг 1.2. Выбор двух взаимно простых больших чисел *p* и *q*, $q < p$.

Шаг 1.3. Определение значения открытого ключа *y* из выражения: $y = q^x \pmod p$.

Шаг 2. Алгоритм шифрования сообщения M.

Шаг 2.1. Выбор случайного числа *k*, удовлетворяющего условию:

$$0 \le k < p\text{-}1 \text{ и } НОД\ (k,p\text{-}1) = 1.$$

Шаг 2.2. Определение значения *a* из выражения: $a = q^k \pmod p$.

Шаг 2.3. Определение значения *b* из выражения: $b = y^k M \pmod p$.

Шаг 2.4. Криптограмма *C*, состоящая из *a и b*, отправляется получателю.

Шаг 2.5. Получатель расшифровывает криптограмму с помощью выражения:

$$M\, a^x = b \ (mod\ p).$$

На рис. 4 представлен результат работы алгоритма шифрования по схеме Эль-Гамаля.

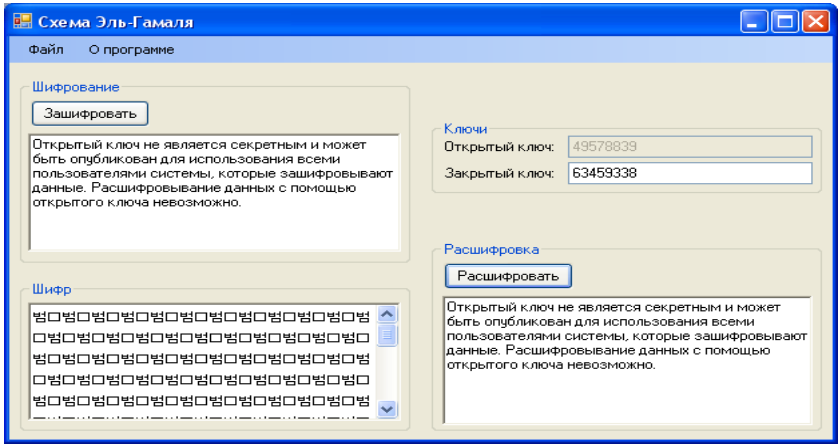

Рис. 4. Алгоритм шифрования по схеме Эль-Гамаля

Задание № 5
Хеш-функция

Цель работы: исследование структуры алгоритмов хеширования: MD5, MD6, CRC, HAVAL, SHA-2, ГОСТ Р 34.11-94.

Задания:

1. Реализовать одну из существующих функций хеширования: MD5, MD6, CRC, HAVAL, SHA-2, ГОСТ Р 34.11-94.

2. Реализовать алгоритм работы функции хеширования на любом языке программирования.

Методика выполнения практической работы. Рассмотреть одну из функций хеширования. Изучить алгоритм работы выбранной функции и после этого реализовать на каком-либо языке программирования.

Требования к работе:

- программа шифрования должна быть наделена понятным и удобным пользовательским интерфейсом;
- полная реализация выбранной функции хеширования.

Основные теоретические положения. Хеширование применяется для сравнения данных: если у двух массивов хеш-функции разные, массивы гарантированно различаются; если одинаковые – массивы, скорее всего, одинаковы. В общем случае однозначного соответствия между исходными данными и хеш-кодом нет в силу того, что количество значений хеш-функций меньше, чем вариантов входного массива; существует множество массивов, дающих одинаковые хеш-коды – так называемые коллизии. Вероятность возникновения коллизий играет немаловажную роль в оценке качества хеш-функций.

Существует множество алгоритмов хеширования с различными характеристиками (разрядность, вычислительная сложность, криптостойкость и т. п.). Выбор той или иной хеш-функции определяется спецификой решаемой задачи. Простейшими примерами хеш-функций могут служить контрольная сумма или CRC. Более детального рассмотрения требует алгоритм хеширования MD5. На рис. 5 изображена схема работы алгоритма MD5.

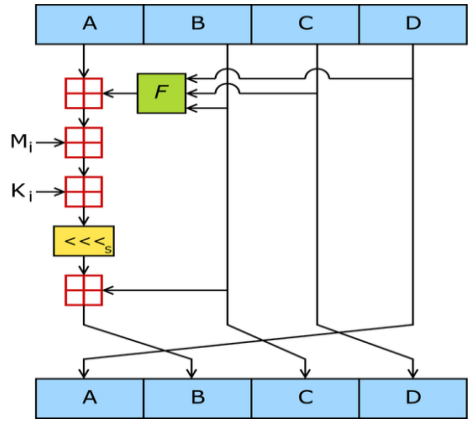

Рис. 5. Схема алгоритма MD5

MD5 – 128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института в 1991 году. Предназначен для создания «отпечатков» или «дайджестов» сообщений произвольной длины. Является улучшенной в плане безопасности версией MD4. Зная MD5, невозможно восстановить входное сообщение, так как одному MD5 могут соответствовать разные сообщения. Используется для провер-

ки подлинности опубликованных сообщений путем сравнения дайджеста сообщения с опубликованным.

На вход алгоритма поступает входной поток данных, хеш которого необходимо найти. Длина сообщения может быть любой (в том числе нулевой). L – длина сообщения. Это число целое и неотрицательное. Кратность каким-либо числам необязательна. После поступления данных идет процесс подготовки потока к вычислениям.

Шаг 0. Выравнивание потока.

Входные данные выравниваются так, чтобы их размер был сравним с 448 по модулю 512 (L' = 512 × N + 448). Сначала дописывают единичный бит в конец потока, затем необходимое число нулевых бит.

Шаг 1. Добавление длины сообщения. В оставшиеся 64 бита дописывают 64-битное представление длины данных (количество бит в сообщении) до выравнивания. Если длина превосходит $2^{64} - 1$, то дописывают только младшие биты. После этого длина потока станет кратной 512. Вычисления будут основываться на представлении этого потока данных в виде массива слов по 512 бит.

Шаг 2. Инициализация буфера. Для вычислений инициализируются 4 переменных сцепления размером по 32 бита и задаются начальные значения шестнадцатеричными числами:

uint A = 0x01234567;
uint B = 0x89ABCDEF;
uint C = 0xFEDCBA98;
uint D = 0x76543210.

В этих переменных будут храниться результаты промежуточных вычислений. Начальное состояние ABCD называется инициализирующим вектором.

Далее определяются функции и константы, которые понадобятся для вычислений.

Требуется 4 нелинейных функции для четырех операций. Вводятся дополнительные функции от трех параметров-слов, результатом также будет слово:

```
private uint funF(uint X, uint Y, uint Z)
{
   return (X & Y) | ((~X) & Z);
}
private uint funG(uint X, uint Y, uint Z)
{
   return (X & Z) | (Y & (~Z));
```

```
}
private uint funH(uint X, uint Y, uint Z)
{
   return X ^ Y ^ Z;
}
private uint funI(uint X, uint Y, uint Z)
{
   return Y ^ (X | (~Z));
}
```

Эти функции спроектированы так, чтобы если соответствующие биты X, Y, Z независимы и не смещены, каждый бит результата также был бы независимым и несмещенным.

Определим таблицу констант T [1… 64] – 64-элементная таблица данных, построенная следующим образом:

$T[i] = int(4294967296 * | sin(i) |)$, где $4294967296 = 2^{32}$.

Выровненные данные разбиваются на блоки (слова) по 32 бита, и каждый блок проходит 4 раунда из 16 операторов. Все операторы однотипны и имеют вид [abcd k s i], определяемый как:

$$a = b + ((a + Fun(b,c,d) + X[k] + T[i]) < < < s),$$

где X – блок данных.

$$X[k] = M [n * 16 + k],$$

где k – номер 32-битного слова из n-го 512-битного блока сообщения, и s – циклический сдвиг влево на s бит полученного 32-битного аргумента.

Шаг 3. Вычисление в цикле. Заносим в блок данных элемент n из массива. Сохраняются значения A, B, C и D, оставшиеся после операций над предыдущими блоками (или их начальные значения, если блок первый).

```
AA = A
BB = B
CC = C
DD = D
```

Этап 1

```
//[abcd k s i] a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s).
[ABCD 0 7 1][DABC 1 12 2][CDAB 2 17 3][BCDA 3 22 4]
[ABCD 4 7 5][DABC 5 12 6][CDAB 6 177][BCDA 7 22 8]
[ABCD 8 7 9][DABC 9 12 10][CDAB 10 17 11][BCDA 11 22 12]
[ABCD 12 7 13][DABC 13 12 14][CDAB 14 17 15][BCDA 15 22 16]
```

Этап 2

//[abcd k s i] a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s).

[ABCD 1 5 17][DABC 6 9 18][CDAB 11 14 19][BCDA 0 20 20]
[ABCD 5 5 21][DABC 10 9 22][CDAB 15 14 23][BCDA 4 20 24]
[ABCD 9 5 25][DABC 14 9 26][CDAB 3 14 27][BCDA 8 20 28]
[ABCD 13 5 29][DABC 2 9 30][CDAB 7 14 31][BCDA 12 20 32]

Этап 3

//[abcd k s i] a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s).

[ABCD 5 4 33][DABC 8 11 34][CDAB 11 16 35][BCDA 14 23 36]
[ABCD 1 4 37][DABC 4 11 38][CDAB 7 16 39][BCDA 10 23 40]
[ABCD 13 4 41][DABC 0 11 42][CDAB 3 16 43][BCDA 6 23 44]
[ABCD 9 4 45][DABC 12 11 46][CDAB 15 16 47][BCDA 2 23 48]

Этап 4

//[abcd k s i] a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s).

[ABCD 0 6 49][DABC 7 10 50][CDAB 14 15 51][BCDA 5 21 52]
[ABCD 12 6 53][DABC 3 10 54][CDAB 10 15 55][BCDA 1 21 56]
[ABCD 8 6 57][DABC 15 10 58][CDAB 6 15 59][BCDA 13 21 60]
[ABCD 4 6 61][DABC 11 10 62][CDAB 2 15 63][BCDA 9 21 64]

Суммируем с результатом предыдущего цикла:

A = AA + A
B = BB + B
C = CC + C
D = DD + D

После окончания цикла необходимо проверить, есть ли еще блоки для вычислений. Если да, то изменяем номер элемента массива (n++) и переходим в начало цикла.

Шаг 4. Результат вычислений. Результат вычислений находится в буфере ABCD, это и есть хеш. Если вывести слова в обратном порядке DCBA, то получится MD5 хеш.

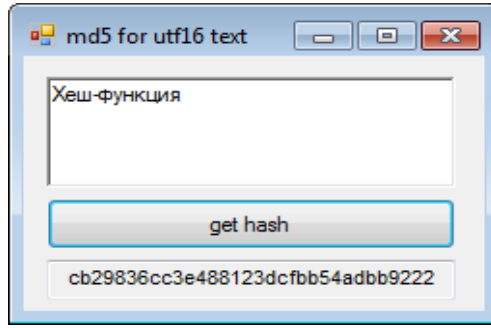

Рис. 6. Форма хеш-функции MD5

На рис. 6 представлен результат работы хеш-функции основанной на алгоритме MD5. Хеш-код строки «Хеш-функция» равен шестнадцатеричному значению:

«cb29836cc3e488123dcfbb54adbb9222».

Задание № 6
Защита программ от несанкционированного копирования

Цель работы: исследование защиты программ от несанкционированного копирования.

Задание:

1. Разработать приложение, которое при установке на другой компьютер выдавало бы сообщение о нелегальности использования.
2. Используя ранее реализованную функцию хеширования, создать хеш-код для строки, содержащей индивидуальную информацию о компьютере; в качестве такой информации должна служить информация о компьютере.

Методика выполнения практической работы. Ознакомиться со способами защиты программ от несанкционированного копирования, способами получения индивидуальной информации о компьютере. Используя результаты практической работы № 4, реализовать защищенное от копирования приложение.

Требования к работе:

- генерируемый хэш-код должен быть привязан к программному и аппаратному обеспечению;
- смена аппаратного и программного обеспечения должна приводить к сообщению о нелегальном использовании программы;
- запрещено использование любых сторонних библиотек.

Основные теоретические положения. Защита от несанкционированного копирования – система мер, направленных на противодействие несанкционированному копированию информации, как правило, представленной в электронном виде (данных или собственнического программного обеспечения). Данная практическая работа основана на привязке компонентов компьютера к серийным номерам. Ее достоинство в том, что не требуется никакого специфического аппаратного обеспечения, и программу можно распространять посредством цифровой дистрибуции. Если пользователь производит модернизацию компьютера, защита отказывает.

В качестве привязки могут использоваться серийный номер BIOS материнской платы, серийный номер винчестера. К этой и по-

добной информации можно обратиться через класс ManagementObjectSearcher находящийся в пространстве имен System.Management.

Задание № 7
Пространство имен Cryptography.NET

Цель работы: исследование пространства имен Cryptography.NET.

Задания:

1. Разработать приложение в среде NET, способное обмениваться по сети информацией, зашифрованной асимметричными алгоритмами шифрования (объекты AsymmetricAlgoritm.DES, AsymmetricAlgoritm.RSA).

2. Организовать возможность добавления цифровых подписей к каждому сообщению с помощью алгоритмов, реализованных в классе HashAlgoritm.

Методика выполнения практической работы. Изучить пространство имен Cryptography.NET. Реализовать на основе полученных знаний приложение для передачи данных по сети.

Требования к работе:

- программа шифрования должна быть наделена понятным и удобным пользовательским интерфейсом;
- обеспечить возможность пресечения попыток обратного проектирования написанного кода;
- организовать передачу шифрованных данных по сети.

Основные теоретические положения. NET Framework включает набор криптографических сервисов, расширяющих аналогичные сервисы Windows через Crypto API. Пространство имен Cryptography открывает доступ к алгоритмам симметричного шифрования. К числу поддерживаемых симметричных алгоритмов относятся DES, RC2, TripleDES. Каждый алгоритм включает какой-нибудь производный от SymmetricAlgorithm абстрактный класс вроде DES и производный от базового управляемый класс или класс провайдера сервиса, например DESCryptoServiceProvider.

Второй тип – асимметричное шифрование или шифрование с открытым ключом. Данный класс является производным от абстрактного класса AsymmetricAlgorithm. К общеизвестным асимметричным алгоритмам относятся DSA и RSA. В асимметричных алгоритмах применяется пара ключей: один – закрытый, другой –

открытый. Как правило, открытый ключ доступен кому угодно и используется отправителем для шифрования данных, тогда как закрытый ключ хранится в защищенном месте и применяется для расшифровки данных, зашифрованных с помощью открытого ключа.

Последний тип алгоритмов, предоставляемых пространством имен Cryptography, связан с хешированием. Алгоритм хеширования вычисляет хэш-код, уникальную последовательность двоичных значений на основе более длинной последовательности байтов. Этот алгоритм позволяет проверять не были ли изменены данные. Если на вход алгоритма хеширования поступают другие данные, на выходе он дает другой результат, и тогда отличие нового хэш-кода от старого указывает на то, что данные изменены. Именно на основе таких алгоритмов обычно реализуются цифровые подписи. Пространство имен Cryptography содержит базовый класс HashAlgorithm и производные классы, поддерживающие алгоритмы MD5, SHA1, SHA256, SHA384 и SHA512. Алгоритм MD5 дает 128-битный кэш, а SHA1 – 160-битный. Числа в названиях других версий SHA-алгоритмов соответствуют длине создаваемых ими хешей.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1. Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации.
2. Основные угрозы информационной безопасности.
3. Основные понятия информационной безопасности.
4. Методы и средства защиты информации.
5. Криптография и стеганография. Основные понятия и определения.
6. Классификация средств криптографической защиты информации.
7. Симметричные алгоритмы шифрования.
8. Ассиметричные алгоритмы шифрования.
9. Ассиметричный алгоритм шифрования, на выбор (RSA, Эль-Гамаля и т. д.).
10. Цифровая подпись. Основные свойства и процедура формирования.
11. Функции хэширования.
12. Идентификация и аутентификация. Основные понятия и классификация.
13. Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак.
14. Критерии и характеристики, учитываемые при сравнении и выборе протоколов аутентификации.
15. Простая аутентификация. Многоразовые пароли, одноразовые пароли.
16. Простая аутентификация. Сертификаты и биометрические характеристики.
17. Строгая аутентификация. Основные понятия.
18. Протоколы аутентификации с нулевой передачей знаний.
19. Защита информационных ресурсов от несанкционированного доступа. Внутримашинные средства.
20. Защита информационных ресурсов от несанкционированного доступа. Дополнительные средства.
21. Защита информационных ресурсов от несанкционированного доступа. Процедуры и методы.
22. Основные угрозы в сетях передачи данных. Основные виды атак в сетях передачи данных.
23. Методы и средства защиты информации в сетях передачи данных.

24. Методы и средства защиты носителей информации.

25. Вредоносные программы. Защита от вредоносных программ.

26. Методы и средства защиты программных продуктов. Вопросы защиты авторского права (имущественные и неимущественные права).

27. Какие цели преследует криптография?

28. Перечислите основные алгоритмы криптографических преобразований.

29. Объясните понятия «целостности, подлинности и конфиденциальности» информации.

30. Перечислите основные методы криптографической защиты информации в компьютерных системах и сетях.

31. Как классифицируются средства криптографической защиты информации?

32. Перечислите основные схемы идентификации пользователя.

33. Назовите основные способы управления ключевой информацией.

34. Назовите два общих принципа, используемых в симметричных криптосистемах.

35. Основные достоинства и недостатки алгоритма шифрования данных с помощью DES.

36. Перечислите основные комбинации, используемые при шифровании алгоритмом DES.

37. Преимущества и недостатки асимметричных криптосистем.

38. С какой целью в асимметричных криптосистемах используются два ключа?

39. Как обеспечивается криптостойкость асимметричных криптосистем?

40. Какова длина ключей для симметричных и асимметричных криптосистем при одинаковой их криптостойкости?

41. Каково основное назначение хеш-функции?

42. Каковы основные принципы формирования хеш-функции?

43. Какими свойствами должна обладать хеш-функция, используемая в процессе аутентификации?

44. Отличительные особенности отечественного стандарта хэш-функции (ГОСТ Р 34.11-94) от алгоритмов хеширования MD5 и SHA.

45. Где и с какой целью используется электронная цифровая подпись?

46. Перечислите основные этапы формирования электронной цифровой подписи.

47. Какими свойствами должна обладать электронная цифровая подпись?

48. Перечислите основные алгоритмы электронной цифровой подписи и укажите на их принципиальные отличия.

49. Укажите особенности слепой и неоспоримой цифровой подписи.

СЛОВАРЬ ТЕРМИНОВ

Авторизация объекта – это процедура предоставления законному объекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Асимметричный шифр – шифр, являющийся асимметричной криптографической системой.

Атака на компьютерную систему (сеть) – это действие, предпринимаемое злоумышленником с целью поиска и использования той или иной уязвимости системы. Таким образом, атака – это реализация угрозы безопасности.

Аутентификация объекта – это проверка подлинности объекта с данным идентификатором. Процедура аутентификации устанавливает является ли объект именно тем, кем он себя объявил.

Безопасная или защищенная система – это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Дешифрование (дешифровка) – процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного. Термин «дешифрование» обычно применяют по отношению к процессу криптоанализа шифротекста (криптоанализ может заключаться и в анализе шифросистемы, а не только зашифрованного ею открытого сообщения).

Достоверность информации – свойство, выражаемое в строгой принадлежности информации субъекту, который является ее источником, либо тому субъекту, от которого она принята.

Доступ к информации – ознакомление с информацией и ее обработка, в частности копирование, модификация или уничтожение. Различают санкционированный и несанкционированный доступ к информации. Санкционированный доступ к информации не нарушает установленные правила разграничения доступа.

Доступность ресурса или компонента системы – это его свойство быть доступным законным пользователям системы.

Идентификация объекта – это процедура распознавания объекта по его идентификатору. Выполняется при попытке объекта войти в систему (сеть).

Избирательная политика безопасности основана на избирательном способе управления доступом. Избирательное, или дискре-

ционное, управление доступом характеризуется задаваемым администратором множеством разрешенных отношений доступа (например, в виде троек <объект, субъект, тип доступа>). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.

Имитовставка – блок информации, применяемый для имитозащиты, зависящий от ключа и данных. В частном случае обеспечивается ЭЦП.

Имитозащита – защита от навязывания ложной информации, достигается обычно за счет включения в пакет передаваемых данных имитовставки.

Информационная безопасность – состояние защищенности обрабатываемых, хранимых и передаваемых данных от незаконного ознакомления, преобразования и уничтожения, а также состояние защищенности информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Ключ – параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах алгоритм шифрования известен, и криптографическая стойкость шифра целиком определяется секретностью ключа (принцип Керкгоффса).

Комплекс средств защиты (КСЗ) представляет собой совокупность программных и технических средств сети. КСЗ создается и поддерживается в соответствии с принятой в данной организации политикой обеспечения информационной безопасности системы.

Комплексный подход ориентирован на создание защищенной среды обработки информации в КС, сводящей воедино разнородные меры противодействия угрозам. Организация защищенной среды обработки информации позволяет гарантировать определенный уровень безопасности КС, что можно отнести к несомненным достоинствам комплексного подхода. К его недостаткам относятся ограничения на свободу действий пользователей КС, чувствительность к ошибкам установки и настройки средств защиты, сложность управления. Комплексный подход применяют для защиты КС крупных организаций или небольших КС, выполняющих ответственные задачи или обрабатывающих особо важную информацию. Нарушение безопасности информации в КС крупных организаций может нанести огромный материальный ущерб как самим организациям, так и их клиентам. Поэтому такие организации вынуждены уделять особое внимание гарантиям безопасности и реализовывать ком-

плексную защиту. Комплексного подхода придерживается большинство государственных и крупных коммерческих предприятий, и учреждений. Этот подход нашел свое отражение в различных стандартах.

Конфиденциальность информации – это ее свойство быть доступной только ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация. По существу, конфиденциальность информации – это ее свойство быть известной только допущенным и прошедшим проверку субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы информация должна быть неизвестной.

Криптоанализ – наука, изучающая математические методы нарушения конфиденциальности и целостности информации.

Криптоаналитик – человек, создающий и применяющий методы криптоанализа.

Криптографическая атака – попытка криптоаналитика вызвать отклонения в атакуемой защищенной системе обмена информацией. Успешную криптографическую атаку называют «взлом» или «вскрытие».

Криптографическая стойкость – способность криптографического алгоритма противостоять криптоанализу.

Криптосистема – семейство обратимых преобразований открытого текста в шифрованный.

Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка – субъекту. На пересечении столбца и строки указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и т. п. Матрица доступа – самый простой подход к моделированию систем управления доступом, однако она является основой сложных моделей, более адекватно описывающих реальные компьютерные системы.

Несанкционированный доступ (НСД) характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями таких правил. Несанкционированный доступ – наиболее распространенный вид компьютерных нарушений.

Оперативность доступа к информации – это способность информации или некоторого информационного ресурса быть до-

ступными конечному пользователю в соответствии с его оперативными потребностями.

Открытый (исходный) текст – данные (не обязательно текстовые), передаваемые без использования криптографии.

Политика безопасности представляет собой набор норм, правил и практических рекомендаций, на которых строятся управление, защита и распределение информации в КС. Политика безопасности регламентирует эффективную работу средств защиты КС. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях.

Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Противодействие угрозам безопасности – цель, которую призваны выполнить средства защиты компьютерных систем и сетей.

Расшифровывание – процесс нормального применения криптографического преобразования шифрованного текста в открытый.

Угрозой безопасности для системы (сети) – возможные воздействия, которые прямо или косвенно могут нанести ущерб ее безопасности.

Ущерб безопасности подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в системе (сети).

Уязвимость системы (сети) – это любая характеристика компьютерной системы, использование которой может привести к реализации угрозы.

«Фрагментарный» подход направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т. п.

Достоинство этого подхода заключается в высокой избирательности к конкретной угрозе. Существенным недостатком его является отсутствие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечивают защиту конкретных объектов КС только от конкретной угрозы. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты.

Целостность информации – свойство сохранять свою структуру и/или содержание в процессе передачи и хранения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, то есть если не произошло их случайного или преднамеренного искажения или разрушения.

Целостность ресурса или компонента системы – это его свойство быть неизменным в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений либо разрушающих воздействий.

Шифрованный (закрытый) текст – данные, полученные после применения криптосистемы с указанным ключом.

Шифрование – процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.

Юридическая значимость информации означает, что документ, являющийся носителем информации, обладает юридической силой.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М., 1989.

2. Гражданский кодекс: федер. закон от 18.12.2006 № 230-ФЗ (ред. 27.12.2018). – URL: http://www.consultant.ru/.

3. Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019). – URL: http://www.consultant.ru/.

4. О персональных данных : федер. закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) – URL: http://www.consultant.ru/.

5. Альманах программиста. NET / сост. Ю. Е. Купцевич. – Т. 4. Безопасность в Microsoft. – М. : Рус. Ред., 2004. – 304 с.

6. Вербицкий, О. В. Вступление к криптологии / О. В. Вербицкий. – Львов : Изд-во наук.-технич. лит., 1998. – 300 с.

7. Гайкович, В. Ю. Безопасность электронных банковских систем / В. Ю. Гайкович, А. Ю. Першин. – М. : Единая Европа, 1994. – 363 с.

8. Гайкович, В. Ю. Основы безопасности информационных технологий / В. Ю. Гайкович. – М. : Инфра-М,1998.

9. Иванов, И. Г. Методические основы защиты информации в банковских автоматизированных комплексах / И. Г. Иванов, П. А. Кузнецов, В. И. Попов // Защита информации. – 1994. – № 1. – С. 13–24.

10. Крат, Ю. Г. Основы информационной безопасности: учеб. пособие / Ю. Г. Крат, И. Г. Шрамкова. – Хабаровск : Изд-во ДВГУПС, 2008. – 112 с.

11. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – 5-е изд. – М. : Академия, 2011. – 330 с.

12. Петраков, А. В. Основы практической защиты информации / А. В. Петраков – М. : Радио и связь, 2001. – 368 с.

13. Проскурин, В. Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в ОС / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. – М. : Радио и связь, 2000. – 166 с.

14. Саломаа, А. Криптография с открытым ключом / А. Саломаа – М. : Мир, 1995. – 318 с.

15. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : учеб. пособие / В. Ф. Шаньгин. – М. : ДМК Пресс, 2008. – 544 с.

16. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

Приложение

ВИДЫ ВРЕДОНОСНЫХ ПРОГРАММ

1. **«Лазейки» (Trapdoors)** обычно инсталлируют во время проектирования системы. Они представляют собой точки входа программы, при помощи которых можно получить непосредственное управление некоторыми системными функциями. Системные программисты организуют лазейки с целью наладить программу и проверить ее возможности. Но после процесса настройки программы их надо устранить. Обнаружить такую лазейку можно в результате анализа работы программ, изучая логику их действия, т. е. проводя аттестацию программ.

2. «**Логические бомбы» (Logic bombs).** «Логическая бомба» является компьютерной программой, которая приводит к повреждению файлов или компьютеров. Повреждение варьируется от искажения данных до полного стирания всех файлов и/или повреждения машины. Логическую бомбу, как правило, инсталлируют во время разработки программы. Она активирует свое действие при выполнении некоторого условия – время, дата, кодовое слово.

3. **«Троянский конь» (Trojan horse)** – это программа, которая приводит к неожиданным (обычно нежелательным) воздействиям на систему. Отличительной характеристикой «троянского коня» является то, что пользователь обращается к ней, считая ее полезной. Эти программы обладают возможностью раскрыть, изменить или уничтожить данные или файлы. «Троянские кони» встраиваются в программах широкого пользования как, например, обслуживание сети, доступные директории, электронная почта и др. В «Оранжевой книге» Национального центра защиты компьютеров США поддерживается список известных «троянских» коней.

4. **«Червяки» (Worms)** – это программы, которые распространяются в системах и сетях по линии связи. Такие программы похожи на вирусы в том, что они заражают другие программы, а отличаются тем, что они не обладают способностью самовоспроизводиться. В отличие от «троянского коня» «червяк» входит в систему без знания пользователя и делает свои копии на рабочих станциях сети.

5. **«Бактерии» (Bacterium).** В терминологию вредительских программ вошло понятие «бактерия». Она представляет собой про-

грамму, которая делает свои копии и становится паразитом, перегружая память и процессор.

6. **«Вирусы» (Viruses).** Определения вирусов бывают весьма разнообразными, как и сами вирусы. Утвердилось определение Ф Коэна: «Компьютерный вирус представляет собой программу, которая способна заражать другие программы, модифицируя их так, чтобы они включали в себя копию вируса (или его разновидность)». В зависимости от области распространения, воздействия, вирусы делятся на разрушительные и неразрушительные, резидентные и нерезидентные, заражающие сектор начальной загрузки, заражающие системные файлы, прикладные программы и др.

Учебное издание

ЗАЩИТА ИНФОРМАЦИИ

Учебно-методическое пособие

Составители:
Гавриленко Тарас Владимирович
Егоров Александр Алексеевич
Еловой Сергей Григорьевич
Гавриленко Анна Владимировна

Редактор Ю. Р. Бобрус

Подписано в печать 25.07.2019. Формат 60×84/16.
Усл.-печ. л. 3,8. Уч-изд. л. 3,1. Тираж 50. Заказ № 72.

Оригинал-макет подготовлен и отпечатан
в Издательском центре СурГУ.
Тел. (3462) 76-30-65, 76-30-66, 76-30-67

БУ ВО «Сургутский государственный университет»
628400, Россия, Ханты-Мансийский автономный округ – Югра,
г. Сургут, пр. Ленина, 1.
Тел. (3462) 76-29-00, факс (3462) 76-29-29.