МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА»

ВЫСШАЯ ШКОЛА ТЕХНОЛОГИИ И ЭНЕРГЕТИКИ

С. Л. Морева

ЗАЩИТА ИНФОРМАЦИИ

Практикум

Санкт-Петербург
2020

УДК 681.3 (07)
ББК 32.98 р
М 793

Морева С.Л. Защита информации: практикум /ВШТЭ СПбГУПТД. – СПб., 2020. – 57 с.

Практикум соответствует программе и учебному плану дисциплины «Защита информации в системах управления и автоматики» для бакалавров, обучающихся по направлению подготовки 27.03.04 «Управление в технических системах». В практикуме собраны упражнения для выполнения практических работ по дисциплине. Приведены методические рекомендации по их выполнению.

Практикум предназначен для подготовки бакалавров очной и заочной форм обучения. Отдельные разделы могут быть полезны специалистам, работающим в области информационной безопасности.

Рецензент:

доцент кафедры ИИТСУ ВШТЭ СПбГУПТД, канд. техн. наук
И.В. Ремизова.

Подготовлен и рекомендован к печати кафедрой информационно-измерительных технологий и систем управления ВШТЭ СПбГУПТД (протокол № 9 от 31.08.2020).

Утвержден к изданию методической комиссией института энергетики и автоматизации ВШТЭ СПбГУПТД (протокол № 2 от 29.10.2020).

Введение

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Формулу успеха любой деятельности в наше время можно сформулировать: кто владеет достоверной и полной информацией – тот владеет ситуацией, а кто владеет ситуацией – тот способен управлять ею в своих интересах, а кто способен управлять – тот способен побеждать. В современном мире нельзя недооценивать вопросы защиты информации. Основные составляющие информационной безопасности любого предприятия или организации: конфиденциальность, целостность, доступность информации. Точками приложения процесса защиты информации к информационной системе являются аппаратное обеспечение, программное обеспечение и обеспечение связи (коммуникации). Разработка механизмов защиты информации любой информационной системы начинается еще на этапе проектирования данной системы. Эти механизмы разделяются на защиту физического уровня, защиту персонала и организационный уровень.

К защищаемой относится информация, которая является предметом собственности и должна защищаться в соответствии с требованиями правовых документов или требованиями, которые устанавливаются собственником.

К информации, требующей защиты, можно отнести конфиденциальную, управленческую, научно-техническую, экономическую и прочую информацию, которая представляет ценность для собственника (предприятия). Утечка такой информации может нанести ущерб ее владельцам в виде экономических убытков, потери имиджа организации и других серьезных упущений. Поэтому необходимо знать и оценивать основные угрозы безопасности информации, уметь оценивать возможные риски.

В эпоху цифровизации особенно актуальна защита информации для промышленных объектов – она является необходимой составляющей обеспечения безопасности. Несанкционированный доступ к управлению технологическими процессами может повлечь за собой серьёзные последствия.

Проблема защиты информации в АСУТП резко обострилась после проведения ряда успешных вирусных атак с использованием вирусного кода программы Stuxnet (2010 г.), когда на иранском заводе по обогащению урана в городе Натанз были разрушены 1000 центрифуг. Позже были обнаружены следующие вредоносные программы: Duqu (2011 г.), Wiper (2012 г.), Flame (2012 г.), Gauss (2012 г.) и MiniFlame (2012 г.). Атака в Иране не единственная, был ряд других, они не приводили к физическим последствиям, но так или иначе дестабилизировали работу различных систем. Один из инцидентов произошёл на Игналинской АЭС, в США были случаи, связанные со сбоями в информационных технологиях, в 2014 г. в результате хакерской атаки произошла утечка чертежей и инструкций по обслуживанию нескольких атомных реакторов энергетической компании Korea Hydro and Nuclear Power, в 2016 г. вредоносное ПО вовремя удалось обнаружить на атомных объектах в Германии, Южной Корее.

Вирусные атаки показали низкую защищенность АСУТП и неготовность противостояния подобным атакам.

Сейчас на отечественных промышленных объектах ведется политика импортозамещения, так как существует риск наличия закладок в оборудовании, комплектующих и программных средствах, поставляемых иностранными производителями.

Иностранные производители осуществляют сервисное (гарантийное) обслуживание с выездом на объект, но при этом не предоставляют российским специалистам доступ к своему оборудованию и ПО. Соответственно возникает возможность внедрения закладок в АСУТП иностранного производства.

Информационная безопасность промышленных объектов – важное направление, которое развивалось по мере распространения интернета и цифровых технологий на промышленных предприятиях.

При этом необходимо понимать, что в промышленности сложно использовать традиционные средства защиты, так как системы имеют другое назначение, свои особенности с точки зрения устойчивости, надёжности, работоспособности. Нельзя просто взять и установить антивирус на программируемые контроллеры или на другие рабочие системы. Необходимо создавать специализированное ПО, которое при этом не наносит вреда оборудованию. Известны случаи, когда антивирусное ПО для корпоративного сегмента может негативно влиять на работоспособность промышленных объектов, излишне потреблять ресурсы, вносить сбои в рабочие процессы и даже останавливать их. Для технологических сегментов такое недопустимо. Поэтому необходимо разрабатывать специализированное ПО, которое затем тщательно тестируется на способность эффективно работать в различных ситуациях и при этом не наносить вреда. Кроме того, в технологическом сегменте больше внимания уделяется пассивным методам детектирования атак, аномалий в технологических системах, сетях, анализу сетевого трафика, направленного не на прерывание подозрительных пакетов, а на уведомление ответственных служб, которые компетентны в принятии решений. Промышленная информационная безопасность также включает не только защиту от проникновения, но и предотвращение утечки критичных данных о процессах и системах, охрану внешнего сетевого периметра организации.

Существует несколько десятков операционных систем для контроллеров. Есть широко распространённые, такие как VxWorks, QNX и др. Антивирусные решения, как правило, не используются внутри операционных систем реального времени. Антивирус требует дополнительных ресурсов. В то же время, если операционная система разработана с учётом анализа киберугроз, она может надёжно работать и без антивируса.

Практикум предназначен для бакалавров, обучающихся по направлению 27.03.04 «Управление в технических системах». Практикум содержит необходимые теоретические сведения и задания для проведения практических работ, необходимые для успешного освоения дисциплины «Защита информации в системах управления и автоматики».

1. Основы информационной безопасности

1.1. Основные понятия информационной безопасности

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

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

Решение проблем информационной безопасности должно начинаться с выявления субъектов информационных отношений и интересов этих субъектов, которые связаны с использованием информационных систем.

Проблемы, связанные с информационной безопасностью, для разных категорий субъектов существенно различаются. Например, проблемы с информационной безопасностью режимного государственного объекта и вуза. В первом случае – это «пусть лучше все сломается, чем враг узнает хоть один секрет», во втором – «да нет у нас никаких секретов, лишь бы все работало».

В различных контекстах с понятием «информационная безопасность» связаны различные определения. Например, в Законе РФ «Об участии в международном информационном обмене» информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. В Доктрине информационной безопасности Российской Федерации указывается, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Оба эти определения рассматривают информационную безопасность в национальных масштабах и поэтому имеют очень широкое понятие.

Рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т. д.), можно утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления – производстве, транспорте и др. Поэтому при определении понятия «информационная безопасность» на первое место ставится защита информации от различных воздействий.

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

Согласно ГОСТ Р 50922-2006 защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Иногда в литературе понятие «информационная безопасность» подменяется термином «компьютерная безопасность». В этом случае информационная безопасность рассматривается очень узко, поскольку

компьютеры – только одна из составляющих информационных систем. В рамках данного практикума основное внимание будем уделять изучению вопросов, связанных с обеспечением режима информационной безопасности применительно к автоматизированным системам управления, в которых информация получается, хранится, обрабатывается и передается с помощью компьютеров.

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

Информационная безопасность – многогранная область деятельности, в которой успех может принести только систематический, комплексный подход.

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

- обеспечением доступности информации;
- обеспечением целостности информации;
- обеспечением конфиденциальности информации.

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

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления – производством, транспортом и т. п. Менее серьезные, но также весьма неприятные последствия (и материальные, и моральные) может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей. Например, продажа железнодорожных и авиабилетов, банковские услуги, доступ в Интернет и т. п.

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

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации н информационных услуг имеют смысл только в определенный промежуток времени. Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно так же получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило. В этом контексте весьма уместной является поговорка: «Дорога ложка к обеду».

Целостность информации условно подразделяется на статическую и динамическую. Статическая целостность информации предполагает неизменность информационных объектов от их исходною состояния, которая определяется автором. Динамическая целостность информации включает вопросы корректного выполнения сложных действий с

информационными потоками: контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, такими как: технические, социальные и т. д.

Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно так же неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, т.е. при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. Конфиденциальность информации есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

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

Все методы защиты информации по характеру проводимых действий можно разделить на:

- законодательные (правовые);
- организационные;
- технические;
- комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации. К таким мерам

относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т.д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты. Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т.е. комплексно.

1.2. Организация работ по обеспечению информационной безопасности в системах управления и автоматики

Существуют определенные требования к персоналу, работающему с АСУТП.

К работе допускаются лица:

– обладающие знаниями и навыками работы в области компьютеризированных систем;

– прошедшие обучение по её аппаратному и программному обеспечению;

– изучившие эксплуатационную и проектную документацию;

– прошедшие обучение по вопросам обеспечения информационной безопасности.

Для АСУТП должны быть определены и применяться основные меры защиты в соответствии с установленной категорией значимости и структурно-функциональными характеристиками системы, обеспечивающие блокирование актуальных угроз ИБ. Эти меры защиты должны поддерживаться в актуальном состоянии.

Доступ к оборудованию и ПО АСУТП должен быть ограничен:

– техническими средствами (наличием замков на шкафах оборудования, ограничением прохода персонала в помещения размещения АСУТП путём установки на дверях механических или электронных кодовых замков);

– организационными мероприятиями (оформление работ нарядом-допуском или распоряжением, допуск к работам с проведением целевого инструктажа, надзор во время работы со стороны ответственных за безопасное проведение работ и ответственного за исправное состояние оборудование, системой паролей/допусков).

В процессе эксплуатации АСУТП оперативным персоналом должен проводиться контроль технического состояния АСУТП согласно инструкциям по эксплуатации. При проведении контроля исправности необходимо учитывать результаты, выдаваемые средствами автоматического контроля работоспособности. Эксплуатационный контроль состояния программного

обеспечения регламентируется соответствующими инструкциями разработчика ПО АСУТП.

При проведении профилактического эксплуатационного контроля запрещается производить какие-либо действия, связанные с изменением программного и аппаратного обеспечения.

Техническое обслуживание АСУТП и регламентные работы с ПО АСУТП должны проводиться в плановом порядке в соответствии с правилами организации технического обслуживания и ремонта систем и оборудования.

Изменение конфигурации аппаратно-программных средств АСУТП может выполняться только в соответствии с процедурами, разработанными и внесёнными в инструкции по эксплуатации систем, и только лицами, ответственными за исправное состояние оборудования.

При возникновении нарушений в работе АСУТП или ситуаций, имеющих признаки инцидента информационной безопасности, персоналу необходимо действовать в соответствии с инструкцией по информационной безопасности предприятия.

1.3. Системный подход к защите информации

Система защиты информации представляет организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

С позиций системного подхода к защите информации предъявляются определенные требования:

– обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле её состояния, выявлений её узких и слабых мест и противоправных действий;

– безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах экономической системы и на всех этапах технологического цикла обработки информации;

– защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить предприятию определенный ущерб;

– методы и средства защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам;

– эффективность защиты информации означает, что затраты на её осуществление не должны быть больше возможных потерь от реализации информационных угроз;

– четкость определения полномочий и прав пользователей на доступ к определенным видам информации;

– предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;

– учет случаев и попыток несанкционированного доступа к

конфиденциальной информации; обеспечение степени конфиденциальности информации;

– обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

2. Законодательство в области информационной безопасности

2.1. Нормативно-правовые документы в области информационной безопасности в РФ

Законодательная база в сфере информационной безопасности состоит из Федеральных законов, Указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов.

На рис. 1 представлены основные нормативно-правовые документы в области информационной безопасности в РФ.

Рис. 1. Нормативно-правовые документы в области информационной безопасности в РФ

Основным законом Российской Федерации является Конституция РФ, принятая 12 декабря 1993 г.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 Конституции гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей; статья 42 – право на знание достоверной информации о состоянии окружающей среды.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; статья 29 – право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение

конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

В Гражданском кодексе Российской Федерации фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

Весьма продвинутым в плане информационной безопасности является Уголовный кодекс Российской Федерации. Глава 28 «Преступления в сфере компьютерной информации» содержит три статьи:

– статья 272. Неправомерный доступ к компьютерной информации;

– статья 273. Создание, использование и распространение вредоносных компьютерных программ;

– статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Первая имеет дело с посягательствами на конфиденциальность, вторая – с вредоносным ПО, третья – с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом компьютерной информации. Включение в сферу действия УК РФ вопросов доступности информационных сервисов является очень актуальным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности информации наиболее полно выражены в законе «О государственной тайне». В нем гостайна определена как защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средствам защиты информации – это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, является закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. номер 149-ФЗ (принят Государственной Думой 8 июля 2006 г.). В нем даются основные определения, намечаются направления, в которых должно

развиваться законодательство в данной области, регулируются отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Статья 16 целиком посвящена вопросам защиты информации. В этой статье Закона фигурируют все три основных аспекта информационной безопасности: доступность, целостность и конфиденциальность. Кроме того, обязательным является отслеживание нарушений безопасности и постоянный контроль за обеспечением уровня защищенности информации.

Президент подписал очень важный закон «Об электронной подписи» номер 63-ФЗ (принят Государственной Думой 6 апреля 2011 г.).

Принят Федеральный закон «О Персональных данных» от 27 июля 2006 г. номер 152-ФЗ (с изм. и доп. 01.03.2021 г.). В статье 2 сформулирована цель Федерального закона: обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Кроме того, хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Основными задачами системы защиты информации, нашедшими отражение в Законе «Об информации, информационных технологиях и о защите информации», являются:

- предотвращение утечки, хищения, утраты, модификации (подделки), несанкционированного уничтожения, искажения, несанкционированного копирования, блокирования информации и т. п., вмешательства в информацию и информационные системы;
- сохранение полноты, достоверности, целостности информации, ее массивов и программ обработки данных, установленных собственником или уполномоченным им лицом;
- сохранение возможности управления процессом обработки, пользования информацией в соответствии с условиями, установленными собственником или владельцем информации;
- обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в банках данных;
- сохранение секретности или конфиденциальности информации в соответствии с правилами, установленными действующим законодательством и другими законодательными или нормативными актами;
- соблюдение прав авторов программно-информационной продукции, используемой в информационных системах.

Законом определено, что средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте РФ, Федеральную службу безопасности РФ и Министерство обороны РФ.

2.2. Ответственность за нарушения в сфере информационной безопасности

Немаловажная роль в системе правового регулирования информационных отношений отводится ответственности субъектов за нарушения в сфере информационной безопасности.

Основными документами в этом направлении являются:

– Уголовный кодекс Российской Федерации.

– Кодекс Российской Федерации об административных правонарушениях.

В Уголовном кодексе Российской Федерации **(**принятом в 1996 г.**)**, как наиболее сильнодействующем законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности, вопросам безопасности информации посвящены следующие главы и статьи:

– Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

– Статья 140. Отказ в предоставлении гражданину информации.

– Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

– Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей.

– Статья 283. Разглашение государственной тайны.

– Статья 284. Утрата документов, содержащих государственную тайну.

Особое внимание уделяется компьютерным преступлениям, ответственность за которые предусмотрена в специальной 28 главе кодекса «Преступления в сфере компьютерной информации» в статьях 272, 273, 274.

Статья 272. Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, – наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы, или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, – наказывается штрафом в размере от ста тысяч

до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, – наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы, или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, – наказываются лишением свободы на срок до семи лет.

Примечания:

– под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи;

– крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ.

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, – наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы, или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, – наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы, или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные

должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, – наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, – наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы, или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, – наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

2.3. Стандарты информационной безопасности

К основным нормативно-правовым документам в области информационной безопасности в РФ, кроме актов федерального законодательства и методических документов государственных органов России, относятся стандарты информационной безопасности.

Стандарт информационной безопасности – нормативный документ, определяющий порядок и правила взаимодействия субъектов информационных отношений, а также требования к инфраструктуре информационной системы, обеспечивающие необходимый уровень информационной безопасности.

ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» является национальным стандартом РФ. Настоящий стандарт идентичен международному стандарту ИСО/МЭК 15408-1:2009. Он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Поэтому этот стандарт часто называют «Общими критериями». В нем определены инструменты оценки безопасности информационных систем и порядок их использования.

«Общие критерии» содержат два основных вида требований безопасности:

– функциональные – соответствуют активному аспекту защиты, предъявляются к функциям безопасности и реализующим их механизмам;

– требования доверия – соответствуют пассивному аспекту, предъявляются к технологии и процессу разработки и эксплуатации.

Угрозы безопасности в стандарте характеризуются параметрами:

– источник угрозы;

– метод воздействия;

– уязвимые места, которые могут быть использованы;

– ресурсы (активы), которые могут пострадать.

Для структуризации пространства требований в «Общих критериях» введена иерархия класс – семейство – компонент – элемент:

– классы определяют наиболее общую, «предметную» группировку требований (например, функциональные требования подотчетности);

– семейства в пределах класса различаются по строгости и другим тонкостям требований;

– компонент – минимальный набор требований, фигурирующий как целое;

– элемент – неделимое требование.

Практическая часть

Задача 1

Используя ГОСТ Р ИСО/МЭК 27002-2012, решить ситуационную задачу.

Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек).

Вам необходимо разработать комплекс мероприятий (от 10 до 20) по следующему направлению: привлечение сторонних организаций к обработке информации.

Цель: обеспечение информационной безопасности при передаче ответственности за обработку информации другой организации.

Изучить разделы ГОСТ Р ИСО/МЭК 27002-2012.

Задача 2

Используя основные положения части 4, главы 70 Гражданского кодекса РФ, решить ситуационную задачу.

Гражданин Смирнов А.В. создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Albert 3D» и зарегистрировал на него свои права. 15.09.2019 этот гражданин заключил договор с компанией «MosTechnology» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «MosTechnology» распространила версию программы «Albert 3D» с предварительной модификацией данного программного продукта без ведома автора.

Вопрос: Имеет ли место в данной ситуации нарушение авторского права гражданина Смирнова?

Ответ: согласно статьи №….

Задача 3

Используя статьи УК РФ, ответьте на вопросы после ознакомления с ситуацией.

Ситуация: А.Н. Иванов, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (расширение .exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 780000 рублей.

Вопросы:

– Какая статья УК РФ была нарушена?
– Что послужило предметом преступления?
– Какие неправомерные информационные действия были совершены А.Н. Ивановым?

Задача 4

Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек).

Вам необходимо разработать требования к хранению, использованию и утилизации информации для вашей организации.

Цель: обеспечение информационной безопасности при хранении, обработке, передаче и уничтожении информации.

Задача 5

Проработайте требования для специалистов по подбору кадров вашей организации с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников.

Цель: уведомление новых сотрудников о строгом выполнении требований по обеспечению информационной безопасности и ответственности за их нарушение.

Контрольные вопросы

1. Перечислите основополагающие документы по информационной безопасности.
2. Понятие государственной тайны.
3. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
4. Дайте характеристику Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных компьютерных программ?
6. Назовите 5 – 6 из 11 существующих функциональных требований стандарта ГОСТ Р ИСО/МЭК 15408-1-2012.
7. Для чего служит профиль защиты, согласно стандарту ГОСТ Р ИСО/МЭК 15408-1-2012?
8. Что прописано в Доктрине информационной безопасности РФ?

9. Чем отличаются функциональные требования от требований доверия, согласно стандарту ГОСТ Р ИСО/МЭК 15408-1-2012?

10. Что предполагает информационное обеспечение любой компании в целом?

3. Организационное обеспечение защиты информации

Организационное обеспечение защиты информации – это регламентация производственной деятельности и взаимоотношений исполнителей, осуществляемая на нормативно-правовой основе таким образом, чтобы сделать невозможным или существенно затруднить разглашение, утечку и несанкционированный доступ к конфиденциальной информации за счет проведения соответствующих организационных мероприятий. Главная цель применения организационных средств защиты – исключить или свести к минимуму возможности реализации угроз информационной безопасности на объектах обработки информации.

Только с помощью организационных мероприятий возможно объединение на правовой основе инженерно-технических, программно-аппаратных, криптографических и других средств защиты информации в единую комплексную систему.

3.1. Классификация угроз информационной безопасности

Угроза информации – это возможность возникновения на каком-либо этапе жизнедеятельности системы такого события, следствием которого могут быть нежелательные воздействия на информацию.

Угрозы информации возникают при нарушении:

- физической целостности (уничтожение, разрушение элементов);
- логической целостности (разрушение логических связей);
- содержания (изменение блоков информации, внешнее навязывание ложной информации);
- конфиденциальности (разрушение защиты, уменьшение степени защищенности информации);
- прав собственности на информацию (несанкционированное копирование, использование).

Три наиболее выраженные угрозы:

- подверженность физическому искажению или уничтожению;
- возможность несанкционированной (случайной или злоумышленной) модификации;
- опасность несанкционированного (случайного или преднамеренного) получения информации лицами, для которых она не предназначена.

По характеру происхождения различают умышленные и естественные факторы.

Умышленные угрозы:

- хищение носителей информации;
- подключение к каналам связи;
- перехват информации;
- несанкционированный доступ;
- разглашение информации;

– копирование данных.

Естественные угрозы:

– несчастные случаи (пожары, аварии, взрывы);

– стихийные бедствия (ураган, наводнение, землетрясение);

– ошибки в процессе обработки информации (ошибки пользователя, оператора, сбои аппаратуры).

Несанкционированный доступ (НСД) – получение лицами в обход системы зашиты с помощью программных, технических и других средств, а также в силу случайных обстоятельств, доступа к обрабатываемой и хранимой на объекте информации.

Разглашение информации ее обладателем – умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшее к не вызванному служебной необходимостью оглашению охраняемых сведений, а также передача таких сведений по открытым техническим каналам.

3.2. Угрозы информационной безопасности в системах управления и автоматики

Компоненты, которые могут быть источником исходных событий нарушения функционирования АСУТП:

– внешняя окружающая среда (стихийные бедствия, техногенные аварии и катастрофы);

– технологическое оборудование (отказы и неисправности аппаратных средств АСУТП, включая нарушение работы системы электропитания);

– человек, деятельность которого непосредственно влияет на информационную безопасность АСУТП и являющийся основным источником угроз;

– смежные информационные системы (отказы);

– обеспечивающие системы АСУТП (отказы);

– отказы систем АСУТП, вызванные ошибками в программном обеспечении и технических средствах АСУТП или закладками в них.

Предпосылки появления угроз:

– объективные (количественная или качественная недостаточность элементов системы) – это причины, не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

– субъективные – причины, непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и

непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

Классификации угроз АСУТП представлена на рис. 2.

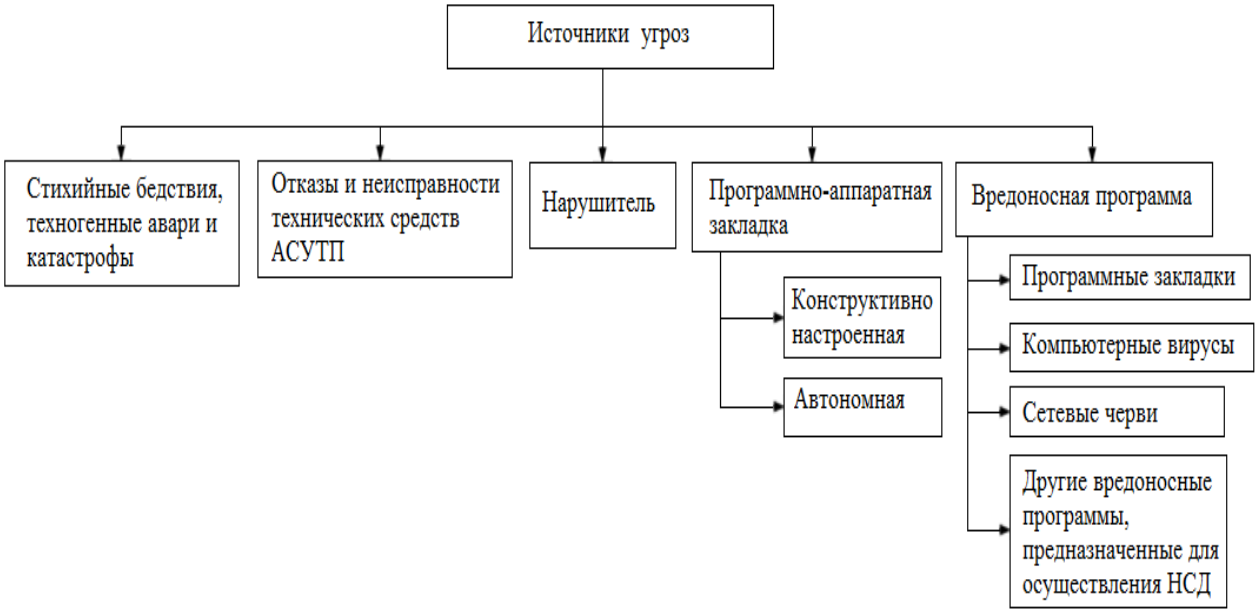

Рис. 2. Структура классификации угроз АСУТП

Подавляющее большинство нарушений физической целостности информации имеет место в процессе ее обработки на различных участках технологических маршрутов. При этом целостность информации зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход. Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов автоматизированных систем обработки данных), которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений автоматизированной системы обработки данных и их оборудования. Что касается злоумышленных действий, то они связаны, главным образом, с несанкционированным доступом к ресурсам автоматизированной системы обработки данных. При этом наибольшую опасность представляет занесение вирусов.

Общая модель процесса нарушения физической целостности информации на объекте автоматизированной системы обработки данных представлена на рис. 3.

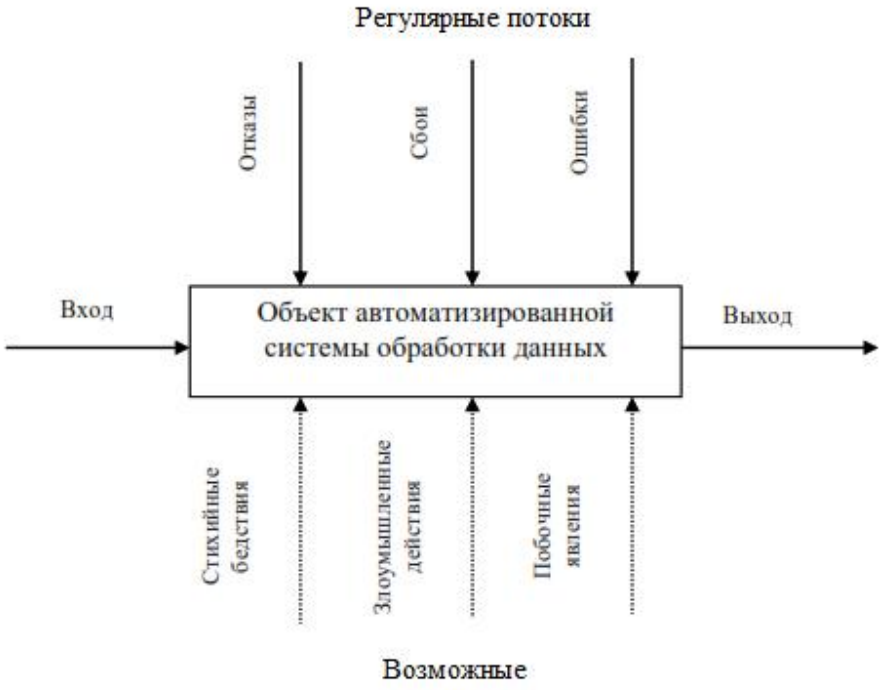

Рис. 3. Общая модель процесса нарушения физической целостности информации

В современных автоматизированных системах обработки данных несанкционированное получение информации возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей. Воздействие случайных факторов непосредственно не ведет к несанкционированному получению информации, оно лишь способствует появлению каналов несанкционированного получения информации, которыми может воспользоваться злоумышленник. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных представлена на рис. 4.

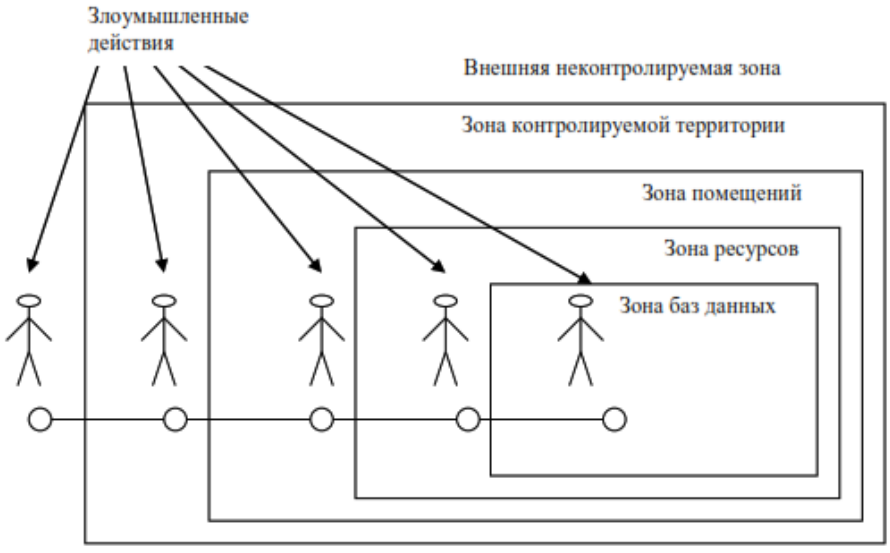

Рис. 4. Структурированная схема потенциально возможных злоумышленных действий

Выделенные зоны определяются следующим образом:

– внешняя неконтролируемая зона – это территория вокруг автоматизированной системы обработки данных, на которой персоналом и средствами автоматизированной системой обработки данных не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации;

– зона контролируемой территории – территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных;

– зона помещений автоматизированной системы обработки данных – внутреннее пространство тех помещений, в которых расположена система;

– зона ресурсов автоматизированной системы обработки данных – та часть помещений, откуда возможен непосредственный доступ к ресурсам системы;

– зона баз данных – та часть ресурсов системы, с которых возможен непосредственный доступ к защищаемым данным.

Злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон. При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий: нарушитель должен получить доступ в соответствующую зону; во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий канал несанкционированного получения информации; соответствующий канал несанкционированного получения информации должен быть доступен нарушителю соответствующей категории; в канале несанкционированного получения информации в момент доступа к нему нарушителя должна находиться защищаемая информации.

Угрозы несанкционированного доступа к информации:

– с использованием программно-аппаратной закладки;

– с использованием уязвимостей ПО (вредоносной программы);

– с использованием уязвимостей протоколов межсетевого взаимодействия;

– с использованием уязвимостей, вызванных недостатками организации работ по обеспечению информационной безопасности АСУТП от несанкционированного доступа;

– с использованием средств информационной безопасности;

– с использованием уязвимостей, вызванных сбоями и отказами программных и аппаратных средств.

Одной из разновидностей теоретически строгих моделей защиты информации являются модели систем разграничения доступа к ресурсам автоматизированной системы обработки данных.

В самом общем виде существо этих моделей может быть представлено следующим образом:

– автоматизированная система обработки данных является системой множественного доступа, т.е. к одним и тем же ее ресурсам (техническим средствам, программам, массивам данных) имеет законное право обращаться некоторое число пользователей (абонентов);

– если какие-либо из указанных ресурсов являются защищаемыми, то доступ к ним должен осуществляться лишь при предъявлении соответствующих полномочий;

– система разграничения доступа и должна стать тем механизмом, который регулирует такой доступ;

– требования к этому механизму на содержательном уровне состоят в том, что, с одной стороны, не должен быть разрешен доступ пользователям (или их процессам), не имеющим на это полномочий, а с другой – не должно быть отказано в доступе пользователям (или их процессам), имеющим соответствующие полномочия.

Практическая часть

Дано пять информационных объектов:

– компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия (отдел кадров);

– компьютер бухгалтера (бухгалтерия);

– личная банковская карта;

– школьный компьютер (компьютерный класс);

– компьютер – рабочая станция оператора (ТЭЦ).

Для каждого из этих объектов указать не менее 7 угроз, которые могут быть реализованы по отношению к обрабатываемой в них информации, а также методы борьбы с данными угрозами.

Обозначить источник каждой из приведенных угроз.

Работу рекомендуется выполнять в таблице вида:

Таблица 1. Рекомендуемый вид таблицы

№ п/п	Наименование угрозы	Источник	Метод защиты от угрозы
Компьютер с конфиденциальной информацией о сотрудниках предприятия			
1.	…	…	…
Банковская карта			
1.	…	…	…
Компьютер бухгалтера			
1.	…	…	…
Компьютер в классе			
1.			
Рабочая станция оператора			
1.			

Контрольные вопросы

1. Что понимается под угрозой информации?
2. Перечислите основные виды угроз.
3. Какова классификация угроз информационной безопасности?
4. Что понимается под термином информационный объект?
5. Назовите источники угроз информационной безопасности.

4. Программно-аппаратное обеспечение защиты информации

4.1. Вредоносное программное обеспечение

Компьютерный вирус – это программа, обладающая способностью к самовоспроизведению и мешающая нормальной работе компьютера.

Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но и могут вообще с ним не совпадать!

Вирус не может существовать в «полной изоляции»: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

Вредоносное программное обеспечение можно разделить на несколько классов по следующим критериям:

- среде обитания;
- способу заражения среды обитания;
- воздействию;
- особенностям алгоритма.

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

- неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;

– опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;

– очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По специфике алгоритма действия различают:

– вирусы-«спутники» – вирусы, которые не изменяют исполняемые файлы, а создают для них файлы-спутники, содержащие их копию;

– «паразитические» – вирусы, которые изменяют содержимое загрузочных секторов диска или файлов;

– макровирус – особая разновидность компьютерных вирусов, которые заражает офисные документы в прикладных программах, имеющих средства и разрешение на исполнения совокупности последовательных команд (макрокоманд);

– троянский конь – компьютерная программа, выполняющая в дополнение к основным не описанные в документации действия при наступлении некоторого условия (даты, времени и т.д.) или по команде извне (например, сбор конфиденциальной информации, рассылка спама и т.д.);

– логическая бомба – особая разновидность компьютерного вируса в виде участка компьютерной программы, который реализует некоторые вредоносные действия при наступлении определенных условий в дате или имени файла;

– стелс-вирус (невидимка) – специально созданная компьютерная программа, которая перехватывает обращения операционной системы или программ к зараженным файлам, секторам носителей информации или оперативной памяти и подставляет вместо себя незараженные участки или содержит так называемые руткиты, позволяющие скрыть деятельность компьютерного вируса;

– полиморфные вирусы (вирусы-призраки) – особая разновидность компьютерного вируса, основное тело которого зашифровано и не имеет постоянного участка программного кода для каждой новой копии;

– бэкдор – компьютерная программа, позволяющая осуществлять скрытое и несанкционированное управление информационной системой извне;

– рекламные системы (adware) – компьютерная программа, инициирующая запуск рекламы или перенаправляющая поисковые запросы на рекламные веб-сайты без ведома и согласия пользователя;

– криптовирусы (ransomware) – особая разновидность компьютерного вируса, который шифрует все файлы определенных типов, найденные на компьютере, после чего удаляет оригиналы.

Практическая часть

Составить характеристику вируса на основе варианта задания. Номером варианта задания является порядковый номер студента в списке группы.

Таблица 2. Варианты задания

Номер варианта	Среда обитания	Способ заражения среды обитания	Способ воздействия	Особенности алгоритма
1	3	2	3	1
2	4	2	1	2
3	3	1	2	3
4	1	2	3	4
5	2	1	1	1
6	4	2	3	2
7	2	1	1	3
8	1	2	2	4
9	4	1	3	1
10	4	2	1	2
11	3	2	2	3
12	2	1	1	4
13	2	1	3	1
14	3	2	1	2
15	3	2	2	3
16	2	1	1	4
17	1	1	3	1
18	1	2	1	2
19	2	1	2	3
20	3	2	1	4
21	1	1	3	1
22	4	2	1	2
23	2	2	2	3
24	3	1	1	4
25	2	1	3	1
26	3	2	1	2
27	4	1	2	3
28	1	2	3	4
29	2	1	1	4
30	1	2	2	3

Классификация вирусов:

По среде обитания:

- сетевые;
- файловые;
- загрузочные;
- файлово-загрузочные.

По способу заражения среды обитания:

- резидентные;
- нерезидентные.

По способу воздействия:

- неопасные;
- опасные вирусы;
- очень опасные.

По особенностям алгоритма:

– макровирусы;
– стелс-вирусы;
– троянский конь;
– бэкдор.

4.2. Восстановление зараженных файлов офисных приложений

Макровирус – это такая разновидность компьютерных вирусов, которая заражает офисные документы в прикладных программах, имеющих средства и разрешение на исполнение последовательных макрокоманд. Макровирусы заражают файлы – документы и электронные таблицы офисных приложений. Для анализа макровирусов необходимо получить текст их макросов. Для нешифрованных (не-стелс) это достигается при помощи меню Сервис/Макрос. Если же вирус шифрует свои макросы или использует стелс-приёмы, то необходимо воспользоваться специальными утилитами просмотра макросов.

Для восстановления документов Word и Excel достаточно сохранить пораженные файлы в текстовом формате RTF, содержащем практически всю информацию из первоначальных документов и не содержащем макросы.

Для этого нужно выполнить следующие действия:

1. В программе WinWord выберите пункты меню «Файл» – «Сохранить как».

2. В открывшемся окне в поле «Тип файла» выберите «Текст в формате RTF» (рис. 5).

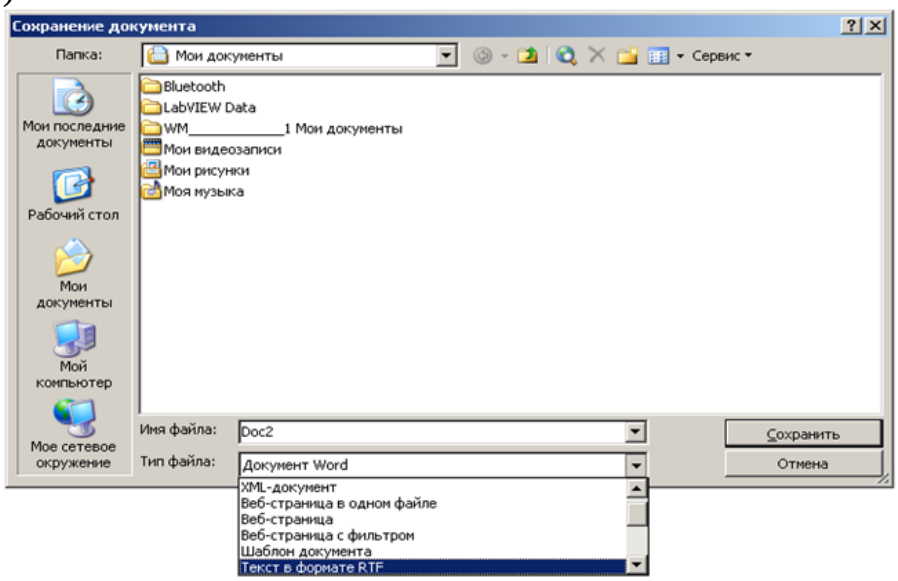

Рис. 5. Выбор формата RTF

3. Выберите команду «Сохранить», при этом имя файла оставьте прежним.

4. В результате появится новый файл с именем существующего, но с другим расширением.

5. Далее закройте WinWord и удалите все зараженные Word-документы и обязательно удалите файл-шаблон Normal.dot в папке WinWord.

6. Запустите WinWord и восстановите документы из RTF-файлов в соответствующий формат файла (рис. 6) с расширением (.doc).

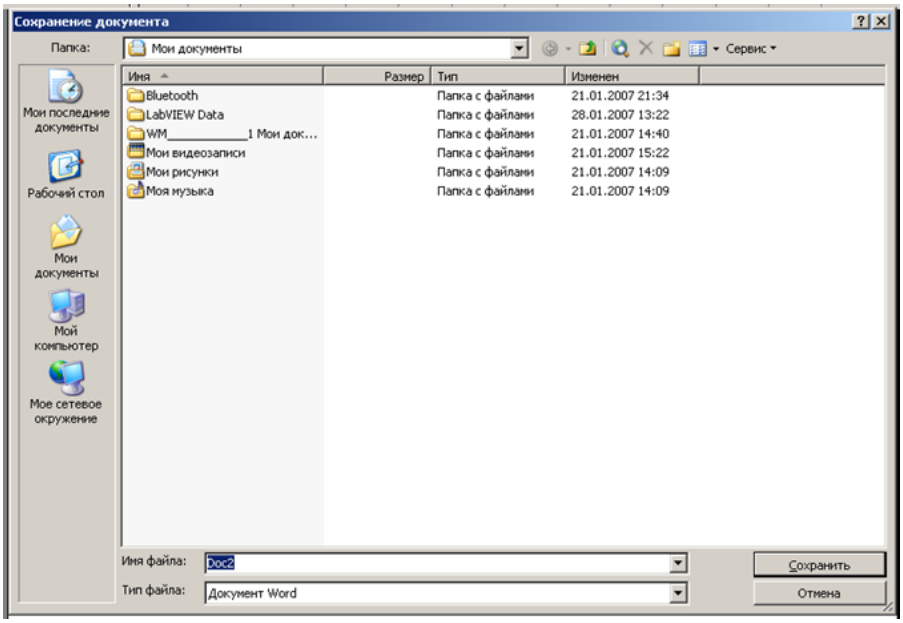

Рис. 6. Восстановление документа с расширением (.doc)

В результате этой процедуры макровирус будет удален из системы, а практически вся информация останется без изменений.

Этот метод рекомендуется использовать, если нет соответствующих антивирусных программ.

При конвертировании происходит потеря невирусных макросов, используемых в данном файле, поэтому перед запуском вышеописанной процедуры рекомендуется сохранить их исходный текст, а после обезвреживания вируса – восстановить необходимые макросы в первоначальном виде.

Для последующей защиты файлов от макровирусов включите защиту от запуска макросов.

Для этого в WinWord выберите последовательно пункты меню: «Сервис» – «Макрос» – «Безопасность» (рис. 7).

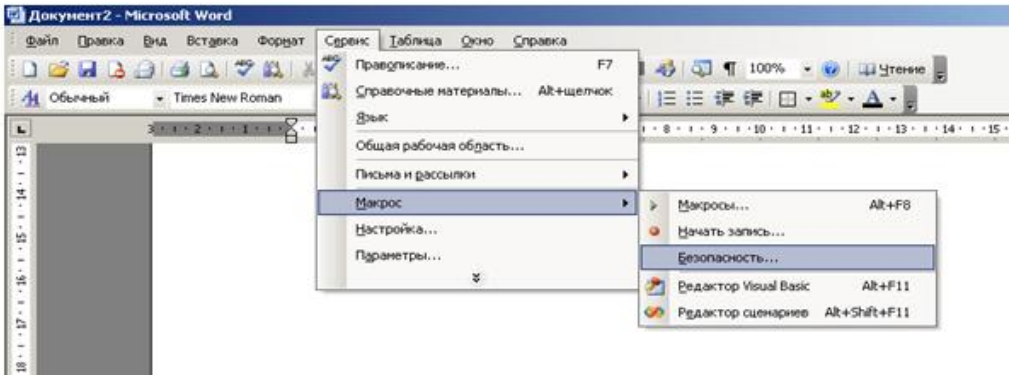

Рис. 7. Выбор меню «Безопасность»

В открывшемся окне на вкладке «Уровень безопасности» отметьте пункт «Очень высокая» (рис. 8).

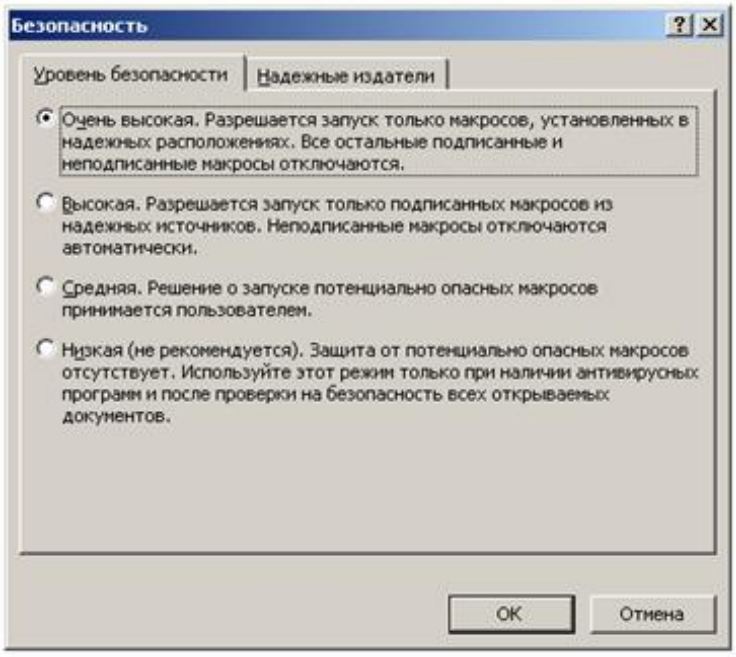

Рис. 8. Выбор пункта «Очень высокая»

Практическая часть

1. Создайте файл virus.doc (содержание – чистый лист) и выполните алгоритм восстановления файла (в предположении его заражения макровирусом).
2. Зафиксируйте этапы работы, используйте команду PrintScreen клавиатуры (скопированные таким образом файлы вставьте в новый Word-документ для отчета).
3. Сравните размеры файлов virus.doc и virus.rtf, используйте пункты контекстного меню «Свойства» (для этого выделите в «Проводнике» файл, нажмите правую кнопку мыши и выберите пункт «Свойства»).

Контрольные вопросы

1. Что такое макровирус?
2. Какие типы файлов заражают макровирусы?
3. Как просмотреть код макровируса?
4. Как восстановить файл, зараженный макровирусом?

4.3. Программы обнаружения и защиты от вирусов

Антивирусная программа (антивирус) – программа, которая пытается обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы с зараженного компьютера, а также служит для профилактики, предотвращения заражения файлов вирусами.

Первые антивирусные программы появились практически сразу после появления первых вирусов. Сейчас разработкой антивирусных программ занимаются крупные компании. Современные антивирусные программы могут обнаруживать десятки тысяч вирусов.

Практически все современные антивирусы не ограничиваются защитой только от вирусов, а детектируют также троянские программы и некоторые другие.

В основу практически всех антивирусов входят:

- ядро;
- сканер;
- монитор активности;
- модуль обновления.

Принцип работы практически всех антивирусов следующий:

- найти и удалить инфицированный файл;
- заблокировать доступ к инфицированному файлу;
- отправить файл в карантин (т.е. не допустить дальнейшего распространения вируса);
- попытаться «вылечить» файл, удалив вирус из тела файла;
- в случае невозможности лечения-удаления, выполнить эту процедуру при следующей перезагрузке операционной системы.

Для того чтобы антивирусная программа постоянно успешно работала, необходимо периодически загружать базу сигнатур вирусов (обычно, через Интернет).

Для успешной зашиты компьютера от вирусов желательно установить один «антивирус» и один «firewall» (сейчас уже есть антивирусные программы, которые предоставляют комплексную защиту, совмещая в себе и то и другое). Если установить больше, то они не смогут работать вместе и это будет вызывать «зависание» компьютера и постоянное торможение, что только ухудшит защиту.

На сегодняшний день список антивирусных программ огромен. Они различаются как по своим функциональным возможностям, так и по цене. Существуют и бесплатные версии антивирусных программ.

Различают следующие виды антивирусных программ:

- программы-детекторы;
- программы-доктора, или фаги;
- программы-ревизоры;
- программы-фильтры, или сторожа;
- программы-вакцины, или иммунизаторы.

Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах, и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора, или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известные из них: Aidstest, Scan, Norton AntiVirus, Doctor Web.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление версий.

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная в России программа Adinf.

Программы-фильтры, или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- попытки коррекции файлов с расширениями COM, EXE;
- изменение атрибутов файла;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако, они не «лечат» файлы и диски. Для уничтожения вирусов требуется применить другие программы, например, фаги. К недостаткам программ-сторожей можно отнести их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением. Наиболее известные программы-фильтры: Outpost, Security Suite, Agnitum Outpost Firewall.

Вакцины, или иммунизаторы – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

Практическая часть

1. Посетить сайты наиболее известных разработчиков антивирусных программ:

– Антивирус Касперского (http://www.kaspersky.ru/),
– Доктор Web (http://www.drweb.com/),
– NOD32 (http: //www.esetnod32.ru/),
– Avast! (http://www.avast-russia.com/).

2. Исходя из информации, представленной на сайтах разработчиков антивирусного ПО, проанализировать виды угроз, от которых гарантированно предоставляется защита. Анализ проводить по параметрам защиты от:

1) мошеннического ПО;
2) хакерских атак;
3) фишинга;
4) спама.

Результаты представить в виде статистической гистограммы, используя средства программного продукта MS Excel.

На основе полученных результатов выбрать антивирусное ПО для реализации политики безопасности компании. Привести обоснование выбора в виде сравнительного отчета выбранного продукта с остальными продуктами по следующим показателям:

а) стоимость;
б) надежность;
в) устойчивость;
г) простота использования;
д) наличие специальных предложений.

3. Изучить настройки антивирусной программы (Антивирус Касперского, DrWeb… – по выбору).

4. Запустите антивирусную программу и выполните проверку оперативной памяти компьютера на наличие вирусов. Выполните тестирование дисков Д: и С: на наличие вирусов. Если на дисках будут обнаружены вирусы, выполните лечение зараженных файлов.

Контрольные вопросы

1. Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы?
2. Повысится ли устойчивость компьютера к воздействию вируса, если установить два антивирусных продукта одновременно?
3. Каковы внешние проявления наличия вируса в компьютере? Приведите примеры широко известных вирусов.
4. Какие программы-доктора вы знаете?
5. Какие вирусы называются резидентными, и в чем особенность таких вирусов?
6. Дать характеристику вируса-невидимки.
7. Что представляет «полная изоляция» вируса?
8. Характеристика сетевых вирусов.
9. Чем опасны файлово-загрузочные вирусы?
10. Что такое логическая бомба?

4.4. Защита информации методом шифрования текста

Шифрование является одним из эффективных способов защиты текстовой информации. При шифровании существуют следующие понятия.

Открытый текст – информация, содержание которой может быть понятно любому субъекту.

Шифрование – процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц. В общем виде процесс шифрования описывается выражением вида $C=E_к(P)$, где C – шифротекст; E – функция шифрования; k – ключ шифрования; P – открытый текст.

Расшифрование – процесс обратного преобразования шифротекста в открытый текст. В общем виде процесс расшифрования описывается выражением вида $P=D_{k'}(C)$, где D – функция расшифрования; k' – ключ расшифрования.

Криптосистема – совокупность алгоритмов, реализуемых функциями E и D, множества ключей k, k' и шифротекстов.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптография (загадочное письмо или тайнопись) – наука о защите информации с помощью шифрования.

В криптографии используются следующие основные алгоритмы шифрования:

– алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;

– алгоритм перестановки – символы шифруемого текста

переставляются по определенному правилу в пределах некоторого блока этого текста;

– гаммирование – символы шифруемого текста складываются с символами в некоторой случайной последовательности;

– аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифровки осуществляются в рамках некоторой криптосистемы. Для симметричной криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровке сообщений. В асимметричных криптосистемах для шифрования данных используется один (общедоступный) ключ, а для расшифровки – другой (секретный) ключ.

Симметричные криптосистемы: шифры простой замены, шифры перестановки, шифры сложной замены (шифр Гронсфельда, гаммирование).

Асимметричные криптосистемы: схема шифрования Эль Гамаля, криптосистема шифрования данных RSA и др.

В данном практикуме подробно рассмотрим шифры простой замены и шифры перестановки. Методы сложного шифрования рассматривать не будем, так как они требуют специальных знаний и теоретической подготовки.

Шифры простой замены

Система шифрования Цезаря – служит примером одной из первых систем шифрования и является частным случаем шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на n букв (Цезарь применял смещение вправо на 3 символа).

Применительно к русскому языку: каждая буква сообщения заменяется на другую, которая в русском алфавите отстоит от исходной на три позиции дальше. Таким образом, буква А заменяется на Г, Б на Д и так далее вплоть до буквы Ь, которая заменяется на Я, затем Э на А, Ю на Б и Я на В.

Рассмотрим пример шифрования поговорки «Под лежачий камень вода не течёт» методом Цезаря.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33			
с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я			

Текст	П	О	Д	Л	Е	Ж	А	Ч	И	Й	К	А	М	Е	Н	Ь	В	О	Д	А	Н	Е	Т	Е	Ч	Ё	Т
Шифротекст	Т	С	Ж	О	З	Й	Г	Ъ	Л	М	Н	Г	П	З	Р	Я	Е	С	Ж	Г	Р	З	Х	З	Ъ	И	Х
Окончательный результат	ТСЖОЗЙГЪЛМНГПЗРЯЕСЖГРЗХЗЪИХ																										

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. По методу перестановки, биты (или символы) открытого текста переставляются в соответствии с заданным ключом шифрования правилом:

$$1 \le i \le n,\ C_i = P_{k[i]}, \qquad (1)$$

где $P = \{P_1, P_2, P_3, \ldots P_i. P_n\}$ – открытый текст; n – длина открытого текста (количество символов текста); $C = \{C_1, C_2, C_3, \ldots C_i. C_n\}$ – шифротекст;

$k = \{k_1, k_2, k_3, \ldots k_i. k_n\}$ – ключ шифрования.

При расшифровании используется обратная перестановка:

$$P_{k[i]} = C_i \qquad (2)$$

Как видно из приведенных выражений, ключ должен удовлетворять условиям: $k_i \neq k',\ 1 \le k' \le n$.

Рассмотрим пример шифрования слова «Сигнал» методом перестановки. Зададим ключ, который должен быть равен 6 символам (количеству символов в шифруемом слове) в виде $k = \{1, 4, 6, 2, 3, 5\}$.

Данные для шифрования:

Символы открытого текста	С	И	Г	Н	А	Л
	P_1	P_2	P_3	P_4	P_5	P_6
Цифровые символы ключа	1	4	6	2	3	5
	k_1	k_2	k_3	k_4	k_5	k_6

Применим формулу (1) с выбранным ключом k к слову «Сигнал». Получим следующие выражения:

$C_1 = P_{k[1]} = P_1 = «с»;$ $C_2 = P_{k[2]} = P_4 = «н»;$

$C_3 = P_{k[3]} = P_6 = «л»;$ $C_4 = P_{k[4]} = P_2 = «и»;$

$C_5 = P_{k[5]} = P_3 = «г»;$ $C_6 = P_{k[6]} = P_5 = «а».$

В конечном итоге получим шифротекст: С = снлига.

Очевидно, что применив другой ключ, получим другой вид шифрованного текста.

При дешифровании используем обратную операцию по формуле (2):

$P_{k[1]} = P_1 = C_1 = «с»;$ $P_{k[2]} = P_4 = C_2 = «н»;$

$P_{k[3]} = P_6 = C_3 = «л»;$ $P_{k[4]} = P_2 = C_4 = «и»;$

$P_{k[5]} = P_3 = C_5 = «г»;$ $P_{k[6]} = P_5 = C_6 = «а».$

Таким образом, получим $P = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ = {сигнал}.

Если требуется зашифровать достаточно длинный текст длиной n, то его можно разбить на блоки, длина которых равна длине ключа m. Открытый текст записывают в таблицу с числом столбцов, равным длине ключа (каждый блок открытого текста записывается в столбец таблицы). Затем столбцы полученной таблицы переставляются в соответствии с ключом перестановки, а шифротекст считывается из строк таблицы последовательно.

Пусть требуется зашифровать открытый текст «студент четвёртого курса». Длина текста (вместе с пробелами $n = 24$). Выберем ключ шифрования в виде:

$k = \{3, 5, 4, 2, 1\}$ $(m = 5)$.

Разбиваем строку «студент четвёртого курса» на пять блоков, каждый из которых располагаем в таблицу:

С	Н	Т	О	У
Т	Т	В	Г	Р
У		Ё	О	С
Д	Ч	Р		А
Е	Е	Т	К	

Переставляем столбцы полученной таблицы в соответствии с ключом $k = \{3, 5, 4, 2, 1\}$. Получим:

Т	У	О	Н	С
В	Р	Г	Т	Т
Ё	С	О		У
Р	А		Ч	Д
Т		К	Е	Е

Считываем последовательно текст из строк таблицы. Получим следующий шифр: *туонс вргтт ёсо ура чдт кее.*

Для расшифровки шифротекст записывают в таблицу того же размера по строкам, затем производится обратная перестановка столбцов в соответствии с

ключом, после чего расшифрованный текст считывается из таблицы но столбцам. Ниже приведены этапы расшифровывания:

а) запись шифротекста в таблицу;

б) перестановка столбцов в соответствии с ключом;

в) считывание символов по столбцам.

Этап а

Т	У	О	Н	С
В	Р	Г	Т	Т
Ё	С	О		У
Р	А		Ч	Д
Т		К	Е	Е

Этап б

С	Н	Т	О	У
Т	Т	В	Г	Р
У		Ё	О	С
Д	Ч	Р		А
Е	Е	Т	К	

Результатом считывания данных таблицы этапа «б» будет фраза «студент четвёртого курса».

Если в качестве ключа перестановки использовать последовательность не цифр, а произвольных символов (например, пароль пользователя), то его необходимо предварительно преобразовать в последовательность целых чисел от 1 до *m*.

Например, пользователь ввел пароль «Москва».

Отсортируем символы в алфавитном порядке, получим: авкмос.

Каждому символу присвоим порядковый номер:

а в к м о с

1 2 3 4 5 6

Заменим символы введённого пароля цифрами и получим ключ: 456321.

Практическая часть

1. Изучить теоретические основы шифрования шифрами простой замены (методом Цезаря и методом перестановки).

2. Зашифровать методом Цезаря предложение открытого текста для шифрования в соответствии с номером своего варианта.

3. Зашифровать (и расшифровать) методом перестановки одно слово открытого текста ключом, длина которого равна длине шифруемого слова. Слово задает преподаватель.

4. Придумать символьный пароль, преобразовать его в ключ и зашифровать (и расшифровать) фразу открытого текста с помощью этого ключа.

Выберите предложение открытого текста для шифрования в соответствии с номером своего варианта (номером по списку группы):

1. От добра добра не ищут.
2. Кто рано встает, тот долго живет.
3. Худой мир лучше доброй драки.
4. Близок локоть, да не укусишь.

5. Жизнь дана на добрые дела.
6. Старый друг лучше новых двух.
7. Сядем рядком да потолкуем ладком.
8. Свято место пусто не бывает.
9. Грамоте учиться всегда пригодится.
10. Доброе слово и кошке приятно.
11. Кто грамоте горазд, тому не пропасть.
12. Дерево познается по его плодам.
13. Из одной печи, да неодинаковы калачи.
14. В чужой монастырь со своим уставом не ходят.
15. Старый дуб не скоро сломится.
16. Кашу маслом не испортишь.
17. На чужой каравай рот не разевай.
18. Доброму совету цены нет.
19. Едешь на день, бери хлеба на неделю.
20. В здоровом теле здоровый дух.
21. Слышал звон, да не знает, где он.
22. Не спеши языком, торопись делом.
23. Всю жизнь живи, всю жизнь учись.
24. Испокон века книга растит человека.
25. Уменье работать дороже золота.
26. Дважды молодым не бывать.
27. Старый конь борозды не портит.
28. Яблоко от яблони недалеко падает.
29. Тише едешь, дальше будешь.
30. На каждый роток не накинешь платок.

Отчет должен содержать подробное описание шифрования и дешифрования с указанием исходного слова (текста), ключа шифрования, символьного и цифрового пароля, результата шифрования (шифротекста).

Контрольные вопросы

1. Что такое ключ?
2. Что такое криптосистема?
3. Пояснить, что такое шифрование и в чём заключается сущность метода Цезаря.
4. Пояснить, в чём заключается сущность метода перестановки.
5. Какие вы знаете основные алгоритмы шифрования?

4.5. Электронная цифровая подпись

В настоящее время повсеместное внедрение информационных технологий отразилось и на технологии документооборота внутри организаций и между отдельными пользователями. Все большее значение в данной сфере

приобретает электронный документооборот, позволяющий отказаться от бумажных носителей (или снизить их долю в общем потоке).

Электронный документ – это любой документ, созданный и хранящийся на компьютере, будь то письмо, контракт или финансовый документ, схема, чертеж, Рис. или фотография.

Электронно-цифровая подпись (ЭЦП) используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью.

ЭЦП – это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;
- конфиденциальность документов;
- установление лица, отправившего документ.

В алгоритмах электронной подписи и асимметричного шифрования используются секретный и открытый ключи. Причем секретный должен браться абсолютно случайно, например, с датчика случайных чисел, а открытый – вычисляться из секретного таким образом, чтобы получить второй из первого было невозможно. Секретный ключ должен тщательно храниться в тайне, ведь любой, кто узнает его, сумеет подделать подпись.

Сейчас существует множество алгоритмов ЭЦП, в том числе:

- национальный стандарт Российской Федерации ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», который обязателен для применения в государственных организациях России и обменивающихся с ними конфиденциальной информацией коммерческих организациях;
- различные общеизвестные алгоритмы ЭЦП, например RSA (Rivest - Shamir – Adleman), Эль-Гамаля, DSA (Digital Signature Algorithm).

Использование ЭЦП позволяет:

- значительно сокращать время, затрачиваемое на оформление сделки и обмен документацией;
- совершенствовать и удешевлять процедуру подготовки, доставки, учета и хранения документов;
- гарантировать достоверность документации;
- минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;
- строить корпоративную систему обмена документами.

Подделать ЭЦП практически невозможно – это требует огромного количества вычислений, которые не могут быть реализованы при современном уровне математики и вычислительной техники за приемлемое время, т.е. пока информация, содержащаяся в подписанном документе, сохраняет актуальность.

Дополнительная защита от подделки обеспечивается сертификацией Удостоверяющим центром открытого ключа подписи.

Согласно действующему законодательству, электронную подпись можно получить путем присоединения данных в электронном виде к другим электронным данным, что служит для идентификации подписанта.

Существует всего три вида электронной подписи:

- простая;
- усиленная неквалифицированная;
- усиленная квалифицированная.

Простая подпись отличается наименьшей степенью защиты информации. Она подтверждает лишь то, что документ был подписан определенным лицом. При этом проверить наличие изменений с момента подписания просто невозможно.

Электронный документ с усиленной неквалифицированной подписью приравнивается к бумажному документу, подписанному человеком. Наличие такой подписи свидетельствует о том, что с момента создания в документ не вносились какие-нибудь правки. Выдают эту подпись специальные центры, которые не проходят аккредитацию.

Квалифицированная ЭП обладает теми же свойствами, что и неквалифицированная подпись, но обязательным ее атрибутом является сертификат ключа проверки ЭЦП.

Простая и неквалифицированная ЭП соответствуют визе на бумажном документе, квалифицированная – это электронная печать и подпись.

Простая ЭЦП (ПЭП) – подпись, состоящая из набора символов и паролей. Ярким примером ПЭП является использование банковской карты. При ее оформлении регистрируется логин и пароль, а при совершении платежных действий абоненту на зарегистрированный в банковской системе телефонный номер приходит код, который следует ввести для подтверждения платежа.

Неквалифицированная ЭП – сведения об абоненте, зашифрованные с использованием криптографического преобразователя информации, которые позволяют отследить подписанта, а также все вносимые в документ изменения после его подписи.

Сделать подпись на компьютере и заверить ею документ можно несколькими способами. Например, электронная подпись создается в документах пакета MS Office. Рассмотрим пример с файлом Word. Чтобы заверить документ, созданный с использованием софта Word, необходимо осуществить следующие действия:

- открываем нужный документ;
- ставим курсор в то место, куда нужно добавить подпись.
- переходим во вкладку «Вставка» и нажимаем кнопку «Строка подписи Microsoft Office» (рис. 9).
- в открывшемся окне заполняем необходимые поля (рис. 10).

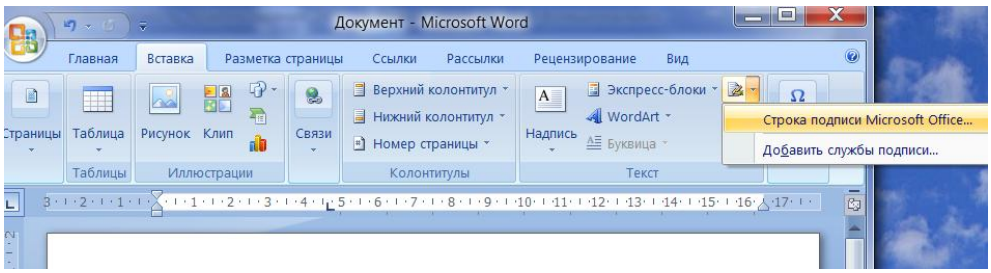

Рис. 9. Выбор кнопки «Строка подписи Microsoft Office»

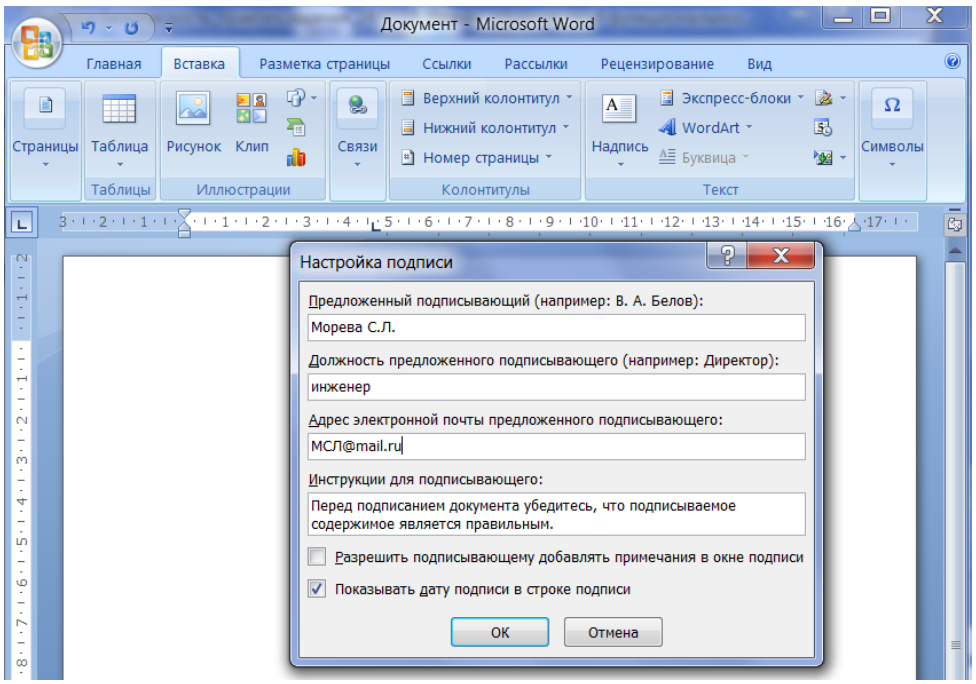

Рис. 10. Заполнение полей настройки подписи

Подпись готова и имеет следующий вид:

X

Морева С.Л.
инженер

Добавить подпись можно и из меню «Файл». Для этого открываем документ, нажимаем кнопки «Файл», «Сведения», «Защита документа» и выбираем функцию «Добавить цифровую подпись».

Далее заполняем форму так же, как в предыдущем примере. Однако подпись, сгенерированную вышеописанным способом, сложно проверить на подлинность.

Способ получения ЭЦП зависит от вида подписи, абонента и нужд, для которых она оформляется.

Процесс подписания документа простой ЭЦП не требует особых знаний. Для этого следует ввести пароль и подтвердить его.

Подписание квалифицированной подписью имеет свои особенности. Перед подписанием документа необходимо установить софт «КриптоПро», софт «Карма» или иной криптографический преобразователь информации и сам

сертификат проверки ключа ЭЦП. Сертификат выдается Удостоверяющим центром при регистрации ЭЦП.

Практическая часть

1. Ответьте на контрольные вопросы.
2. Заверьте свою работу электронной подписью.
3. Зафиксируйте этапы работы, используя команду PrintScreen.

Контрольные вопросы

1. Что такое электронно-цифровая подпись?
2. Для чего используется механизм электронной цифровой подписи?
3. Алгоритмы электронно-цифровой подписи.
4. Какой метод шифрования использует электронная цифровая подпись?
5. Виды цифровой подписи.

4.6. Профилактика проникновения в ОС WINDOWS 10 «троянских программ»

«Троянские программы» («Троянский конь») – это вредоносное программное обеспечение. Рассмотрим потенциальные места записей «троянских программ» в определенные разделы системного реестра.

Реестр операционной системы Windows 10 – это большая база данных, где хранится различная информация о конфигурации системы. Этой информацией пользуются, как операционная система Windows 10, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого необходимо иметь копию реестра. Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «Редактор реестра».

Программа редактора реестра находится в папке C:\Windows. Называется программа regedit.exe, существует также более новая версия редактора реестра regedt32.exe. После запуска появится окно редактора реестра. Вы увидите список из пяти разделов (рис. 11).

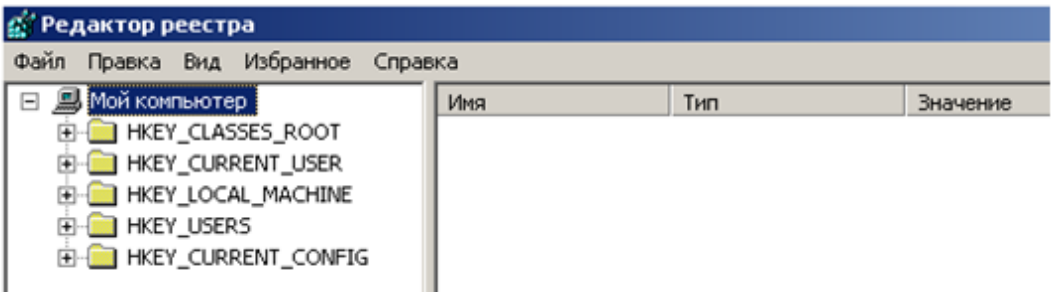

Рис. 11. Окно редактора реестра

Также открыть реестр можно нажав комбинацию клавиш Windows+R и в появившемся окне ввести regedit и нажать OK.

Работа с разделами реестра аналогична работе с папками в проводнике. Конечными элементом дерева реестра являются ключи или параметры, которые делятся на три типа (рис. 12):

– Строковые (например «C:\Windows»);

– Двоичные (например 10 87 A0 8D);

– DWORD – этот тип ключа занимает 4 байта, отображается в десятичном и шестнадцатеричном виде (например 0X00000020 (32)).

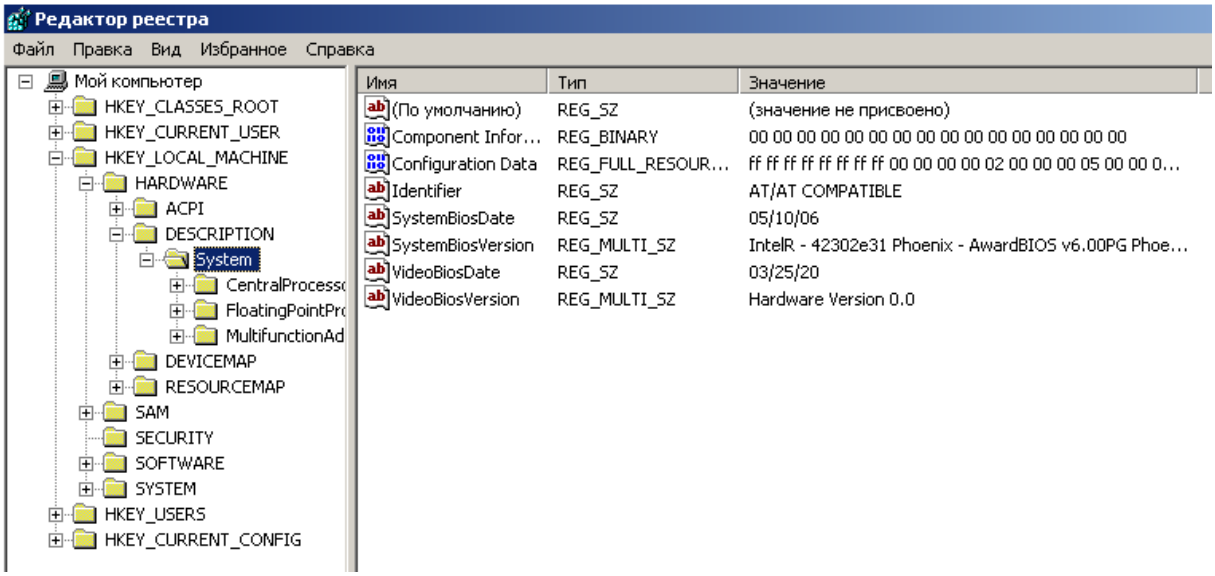

Рис. 12. Типы параметров редактора реестра

В Windows 10 системная информация в реестре разбита на так называемые ульи (hive). Это обусловлено принципиальным различием концепции безопасности ОС Windows. Имена файлов ульев и пути к каталогам, в которых они хранятся, расположены в разделе:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist (рис. 13).

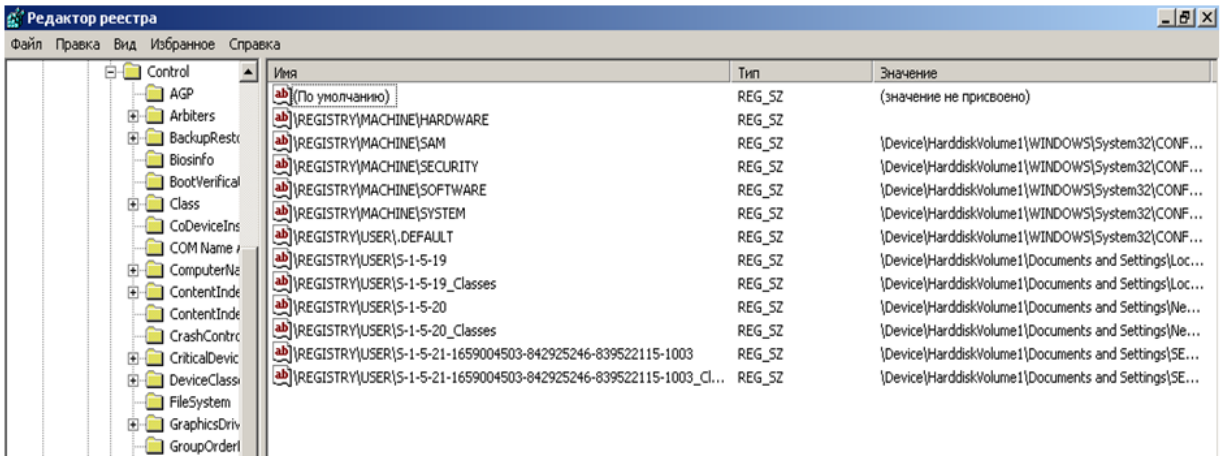

Рис. 13. Имена файлов ульев и пути к каталогам

В табл. 3 даны краткие описания ульев реестра и файлов, в которых хранятся параметры безопасности.

Таблица 3.

Характеристика основных разделов системного реестра ОС Windows 10

Раздел системного реестра	Характеристика
HKEY_LOCAL_MACHINE\SAM	Содержит информацию SAM (Security Access Manager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке %Systemroot%\System32\Config
HKEY_LOCAL_MACHINE\SECURITY	Содержит информацию безопасности в файлах SECURITY, SECURITY.LOG, SECURITY.SAV в папке %Systemroot%\System32\Config
HKEY_LOCAL_MACHINE\SYSTEM	Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлах SYSTEM, SYSTEM.LOG, SYSTEM.SAV в папке %Systemroot%\System32\Config
HKEY_CURRENT_CONFIG	Содержит информацию о подразделе SYSTEM этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке %Systemroot%\System32\Config
HKEY_USERS\DEFAULT	Содержит информацию, которая будет использоваться для создания профиля нового пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке %Systemroot%\System32\Config
HKEY_CURRENT_USER	Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT, NTUSER.DAT.LOG, расположенных в каталоге \%SYSTEM%\Profiles\Username, где User name – имя пользователя, зарегистрированного в системе на данный момент

Практическая часть

1. Проверить потенциальные места записей «троянских программ» в системном реестре ОС Windows 10.

2. Проверить содержимое ключа:

HKEY_LOCAL_MACHINE\Software\Microsoft\ WindowsNT\CurrentVersion\Winlogon\System(REG_SZ).

3. Зафиксировать этапы работы, используя команду PrintScreen.

4. Составить отчет о результатах проверки.

Методические рекомендации по выполнению работы

Потенциальными местами записей «троянских программ» в системном реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.

1. Запустите программу regedit.exe.

2. В открывшемся окне выберите ветвь HKEY_LOCAL_MACHINE и далее Software\Microsoft\WindowsNT\CurrentVersion\Winlogon.

3. В правой половине открытого окна программы regedit.exe появится список ключей.

4. Найдите ключ Userinit (REG_SZ) и проверьте его содержимое.

5. По умолчанию (исходное состояние) 151, этот ключ содержит следующую запись C:\WINDOWS\system32\userinit.exe (рис. 14).

6. Если в указанном ключе содержатся дополнительные записи, то это могут быть «троянские программы».

7. В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла и сопоставьте с вашими действиями в это же время.

8. Если время создания файла совпадает со временем работы в сети Internet, то возможно, что в это время компьютер был заражен «троянской программой».

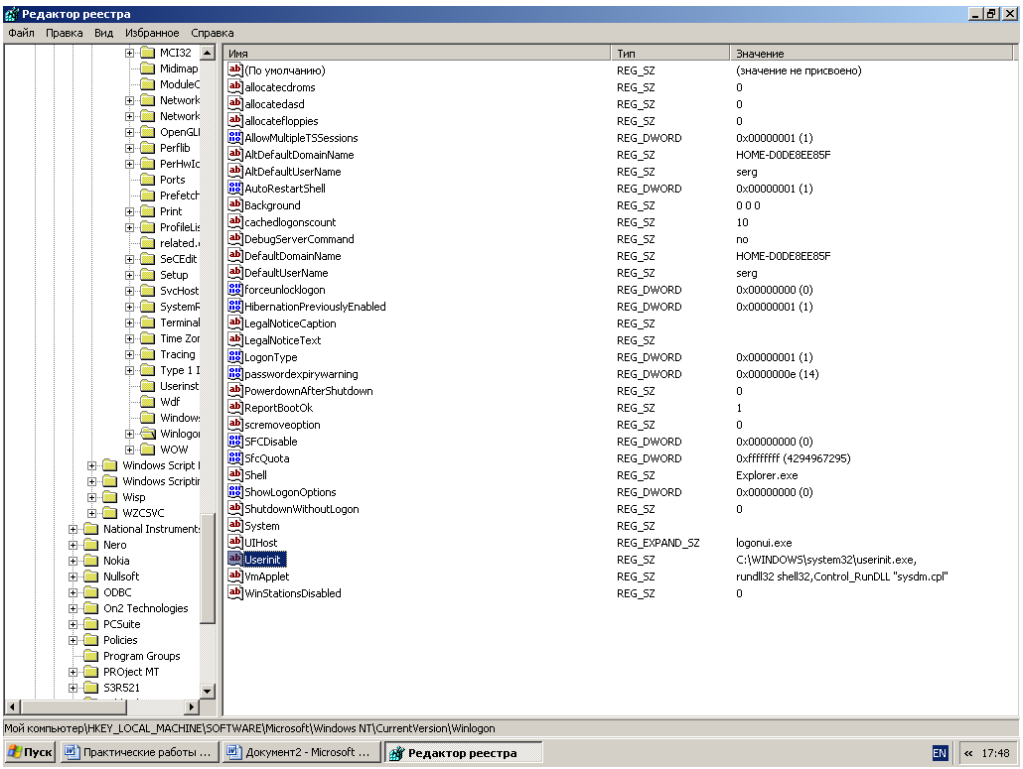

Рис. 14. Содержимое ключа Userinit (REG_SZ)

9. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду «Изменить» из меню «Правка» программы regedit.exe).

10. В открывшемся поле значение (рис. 15) удалите ссылку на подозрительный файл.

11. Закройте программу regedit.exe.

12. Перейдите в папку с подозрительным файлом и удалите его.

13. Перезагрузите операционную систему и выполните 1-4 пункты задания.

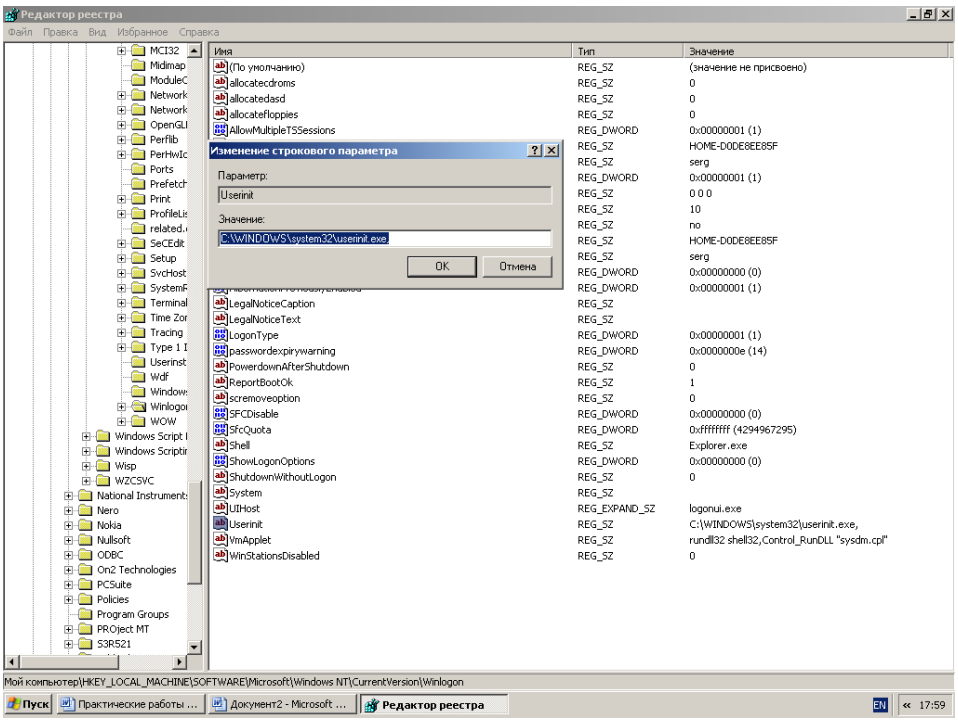

Рис. 15. Удаление ссылки на подозрительный файл

14. Если содержимое рассматриваемого ключа не изменилось, то предполагаемая «троянская программа» была удалена из вашей системы.

Ещё одним потенциальным местом записей на запуск «троянских программ» является раздел автозапуска Run.

Для его проверки выполните следующее:

1. Запустите программу regedit.exe.

2. В открывшемся окне выберите ветвь HKEY_LOCAL_MACHINE и далее Software\Microsoft\Windows\CurrentVersion\Run\.....(REG_SZ) (рис. 16).

3. В рассматриваемом примере запускаются различные программы, просмотрите вашу ветвь, запускаемые программы занесите в отчет, прокомментируйте, выясните их месторасположение.

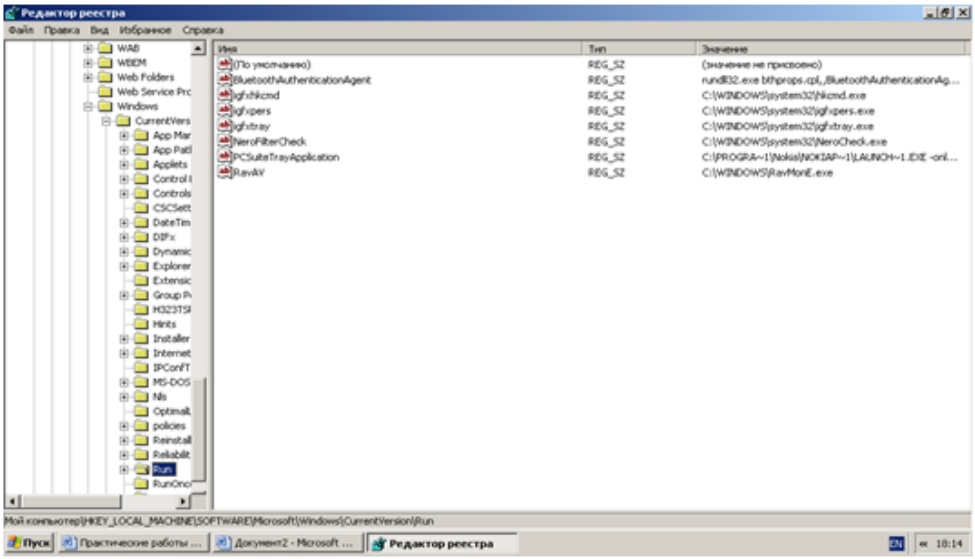

Рис. 16. Раздел автозапуска Run

Контрольные вопросы:

1. Что такое реестр ОС Windows 10?
2. Поясните особенности «троянских программ».
3. Почему профилактика «троянских программ» связана с системным реестром?
4. Какие разделы и ключи реестра являются потенциальными местами запуска «троянских программ»?

4.7. Аутентификация и идентификация

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и/или идентификации. Идентификация и аутентификация применяются для ограничения доступа случайных или незаконных субъектов (пользователей, процессов) к информационной системе, объектам-ресурсам (аппаратным, программным, информационным).

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он сам себя выдаёт.

Настройка параметров аутентификации в ОС Windows 10 выполняется в рамках локальной политики безопасности. Вкладка «Локальная политика безопасности» используется для изменения политики учетных записей и локальных политик безопасности на компьютере. При помощи вкладки «Локальная политика безопасности» можно определить:

- кто имеет доступ к компьютеру;
- какие ресурсы могут использовать пользователи на компьютере;
- включение и выключение записи действий пользователей или группы пользователей в журнале событий.

Практическая часть

1. Настройте параметры локальной политики безопасности операционной системы Windows 10.
2. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль.
3. После успешного выполнения предыдущего задания измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

4. Проведите эксперименты с другими параметрами «Политики учетных записей».

Методические рекомендации по выполнению работы

Для просмотра и изменения параметров аутентификации пользователей выполните следующие действия:

1. Выберите кнопку «Пуск» на панели задач.
2. Откройте меню «Настроить» – «Панель управления».
3. В открывшемся окне выберите ярлык «Администрирование» – «Локальная политика безопасности» (рис. 17).

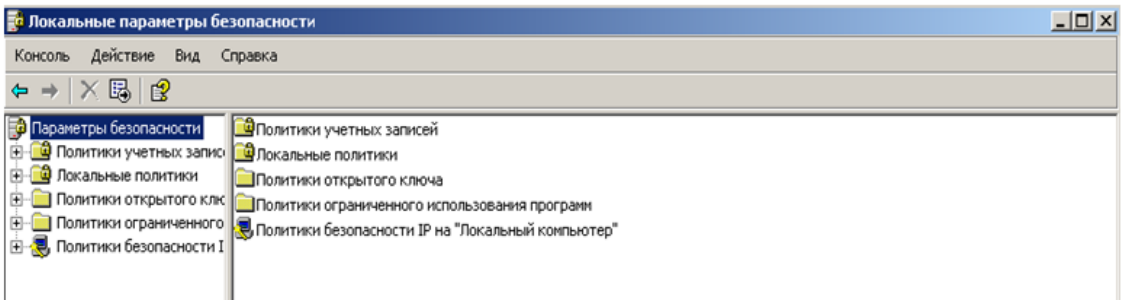

Рис. 17. «Локальная политика безопасности»

4. Выберите пункт «Политика учетных записей». Этот пункт включает два подпункта: «Политика паролей» и «Политика блокировки учетной записи».
5. Откройте подпункт «Политика паролей». В правом окне появится список настраиваемых параметров (рис. 18).

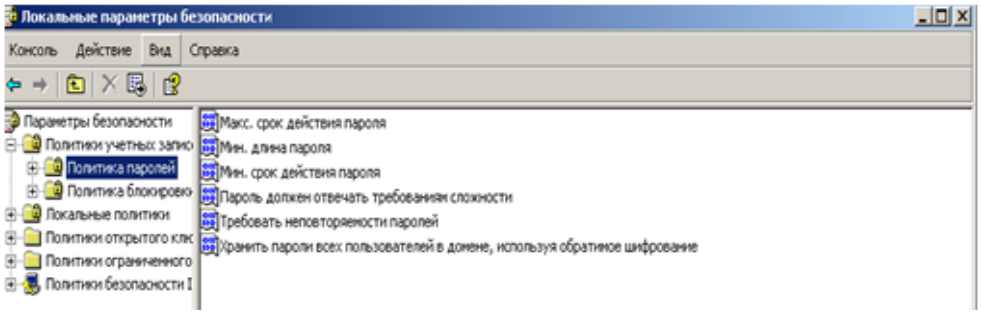

Рис. 18. Список настраиваемых параметров

6. В показанном примере политика паролей соответствует исходному состоянию системы безопасности после установки операционной системы, при этом ни один из параметров не настроен. Возможные значения параметров приведены в табл. 4.

Таблица 4. Параметры «Политики паролей»

Параметр	Значение
Требовать повторяемости паролей	Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24

Окончание табл. 4

Параметр	Значение
Максимальный срок действия пароля	Определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0
Минимальный срок действия пароля	Определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0
Минимальная длина пароля	Определяет наименьшее число символов, которое может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов равным 0
Пароль должен отвечать требованиям сложности	Определяет, должны ли отвечать пароли требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям: – Пароль не может содержать имя учетной записи пользователя или какую-либо его часть; – Пароль должен состоять не менее чем из 6 символов; – В пароле должны присутствовать символы трех категорий из числа следующих: 1. Прописные буквы английского алфавита от A до Z; 2. Строчные буквы английского алфавита от A до Z; 3. Символы, не принадлежащие алфавитно-цифровому набору (например, !,$,#,%). Проверка соблюдения этих требований выполняется при изменении или создании паролей
Хранить пароли всех пользователей в домене, используя обратимое шифрование	Определяет, следует ли в системе Windows 10 хранить пароли, используя обратимое шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранить пароли, зашифрованные обратимыми методами, это всё равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля

7. Ознакомьтесь со свойствами всех параметров.

8. Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды щёлкните на изменяемом параметре).

9. В результате этого действия появится одно из окон, показанных на рис. 19, 20.

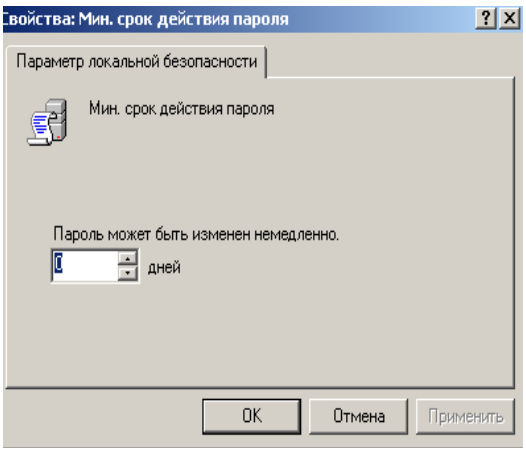

Рис. 19. Изменение срока действия пароля

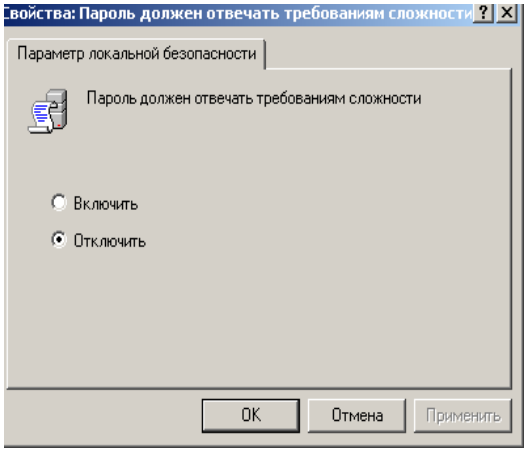

Рис. 20. Изменение настраиваемых параметров

10. Измените, значение параметра и нажмите Ок.

11. Например, «обязательно выполнить и сохранить», выберите параметр «Требовать неповторяемости паролей» и измените его значение на 1.

12. Для настройки «Политики блокировки учетной записи» выберите этот подпункт и откройте его.

13. Значения параметров данного подпункта «Политики блокировки учетной записи» приведены в табл. 5.

Таблица 5. Параметры «Политики блокировки учетной записи»

Параметр	Значение
Пороговое значение блокировки	Определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока блокировка не будет сброшена администратором или пока не истечёт её интервал блокировки. Можно задать значение в диапазоне от 1 до 999 или запретить блокировку данной учетной записи, установив значение 0

Окончание табл. 5

Параметр	Значение
Блокировка учетной записи на	Определяет число минут, в течение которых учетная запись остаётся блокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 1 до 99999 мин. Если установить значение 0, учетная запись будет блокирована на всё время до тех пор, пока администратор не разблокирует её явным образом. Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса
Сброс счетчика блокировки через	Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99999 мин. Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше интервала Блокировка учетной записи на

14. Ознакомьтесь со свойствами всех параметров.

15. Для изменения параметров воспользуйтесь алгоритмом, описанным в пунктах 8-10.

Контрольные вопросы:

1. Что такое аутентификация и идентификация?
2. Для чего применяются эти механизмы?
3. Что можно настроить с помощью вкладки «Локальные политики безопасности»?

Заключение

В эпоху цифровизации защита информации промышленных объектов стала необходимой составляющей обеспечения безопасности, так как несанкционированный доступ к управлению технологическими процессами может повлечь за собой серьёзные последствия.

Системы управления больше не защищены за счёт закрытости объекта, как это было раньше. Мы теперь работаем и в корпоративных сетях, и в сетях систем управления с использованием одной и той же рабочей станции. Количество кибератак в промышленности не будет уменьшаться, ведь сегодняшний тренд – цифровизация. И она будет проникать всё глубже, охватывая новые сферы. Промышленная индустрия 4.0, умные города и прочие подобные программы – вот современные мировые тренды. При этом цифровизация не только даёт новые возможности, но и влечёт за собой новые потенциальные угрозы. Даже появилась такая шутка: «Если умный, значит – небезопасный».

На промышленных объектах проводят диагностику на уязвимость. Анализируют защищённость методом тестов на проникновение, методом аудита, анализа конфигурации и другими способами. Тест – это попытка моделирования действий атакующего, аудит – это сбор данных, опрос, чтение конфигураций, изучение документации. В результате выявляются недостатки в технологических процессах, в бизнес-процессах, в документации, в конфигурации оборудования, которые могут привести к уязвимости ПО. Уязвимости находят у многих производителей, даже таких известных, как Schneider Electric и Siemens. Угрозы информационной безопасности в будущем никуда не исчезнут, но и технологии, связанные с промышленной информационной безопасностью, также неизбежно будут развиваться, отвечая вызовам современного цифрового мира.

Поэтому крайне актуальной является подготовка специалистов в области защиты информации.

Библиографический список

Конституция РФ (http://constitutionrf.ru/).

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». (http://base.garant.ru/l2148555/).

Гражданский кодекс РФ Ч. 4. Раздел 7 «Права на результаты интеллектуальной деятельности и средства индивидуализации» (от 18 декабря 2006 г. № 230-ФЗ). (http://www.consultant.ru/document/cons doc LAW 64629/).

Доктрина информационной безопасности РФ (утверждена указом Президента РФ № 646 от 5 декабря 2016 г.). (https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html).

ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. (http://docs.cntd.ru/document/1200103619).

Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. – СПб: Лань, 2019. – ISBN 978-5-8114-3940-9. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/l 25739 (дата обращения: 07.11.2020).

Жук, А. П. Защита информации: учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 2-е изд. – М.: РИОР: ИНФРА-М, 2017. – 392 с. – Режим доступа: http://znanium.com/bookread2.php?book=937469.

Краковский, Ю.М. Защита информации [Электронный ресурс]: учеб. пособие / Ю.М. Краковский. – Электрон. текстовые данные. – Ростов-на-Дону: Феникс, 2016. – 349 с. – Режим доступа: http://www.iprbookshop.ru/59350.html.

Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ О.В.Прохорова. – Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. – 113 с. – (ЭБС «IPRbooks»: Режим доступа: http://www.iprbookshop.ru/43183).

Гришина, Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. – 2-е изд., доп. – М. : Форум: НИЦ ИНФРА-М, 2015. – 240 с.: ил.; . – (Высшее образование: Бакалавриат). ISBN 978-5-00091-007-8. – Текст : электронный. – URL: https://znanium.com/catalog/product/491597 (дата обращения: 27.10.2020).

Содержание

Учебное издание

Светлана Леонидовна Морева

ЗАЩИТА ИНФОРМАЦИИ

Практикум

Редактор и корректор Н.П. Новикова
Техн. редактор Л.Я. Титова Темплан 2020 г., поз. 145

Подп. к печати 30.03.21 Формат 60х84/16. Бумага тип. № 1.
Печать офсетная. Печ.л. 3,75 Уч.-изд. л. 3,75.
Тираж 50 экз. Изд. № 145 Цена «С». Заказ

Ризограф Высшей школы технологии и энергетики СПбГУПТД,
198095, СПб., ул. Ивана Черных, 4.