Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
сборник учебно-методических материалов

для направления подготовки 01.03.02 Прикладная математика и информатика

Благовещенск

2017

Печатается по решению
редакционно-издательского совета
факультета математики и информатики
Амурского государственного
университета

Составитель: Самохвалова С.Г.Фомин Д.В.

Методы защиты информации: сборник учебно-методических материалов для направления подготовки 01.03.02 Прикладная математика и информатика – Благовещенск: Амурский гос. ун-т, 2017. – 90 с.

КРАТКОЕ ИЗЛОЖЕНИЕ ЛЕКЦИОННОГО МАТЕРИАЛА

Введение.

Современный этап развития человечества, вступившего в эпоху глобального перехода к «информационному обществу», характеризуется проникновением компьютерных технологий во все сферы человеческой деятельности и, как следствие, обострением проблемы обеспечения информационной безопасности.

В соответствии с Федеральным законом РФ «Об информации, информационных технологиях и о защите информации» под *информацией* принято понимать сведения (сообщения, данные) независимо от формы их представления.

Для более глубокого понимания проблемы информационной безопасности определим ещё два понятия: безопасность информации и защита информации.

Понятие «*безопасность информации*» распадается на две составляющие:

1) *безопасность содержательной части* (*смысла*) *информации* - отсутствие в ней побуждения человека к негативным действиям, умышленно заложенных механизмов негативного воздействия на человеческую психику или негативного воздействия на иной блок информации (например, информация, содержащаяся в программе для ПК, именуемой компьютерным вирусом);

2) *защищённость информации от внешних воздействий* (попыток неправомерного копирования, распространения, модификации (изменения смысла) либо уничтожения).

Вторую составную часть понятия «*безопасность информации*» предлагается называть *защитой информации*.

Однако защите подлежит не всякая информация, а только та, которая имеет цену. *Ценность информации* определяется степенью её полезности для владельца. Обладание истинной (достоверной) информацией даёт её владельцу определённый выигрыш: моральный, материальный, политический и т.д. Ценность информации является критерием при принятии любого решения о её защите и выборе метода защиты.

В соответствии с *Законом об информации* (*статья 5*) вся информация в зависимости от категории доступа к ней подразделяется на *общедоступную информацию*, а также на информацию, доступ к которой ограничен федеральными законами (*информация ограниченного доступа*) (рис. 11.1).

Информация в зависимости *от порядка ее предоставления* или *распространения* подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

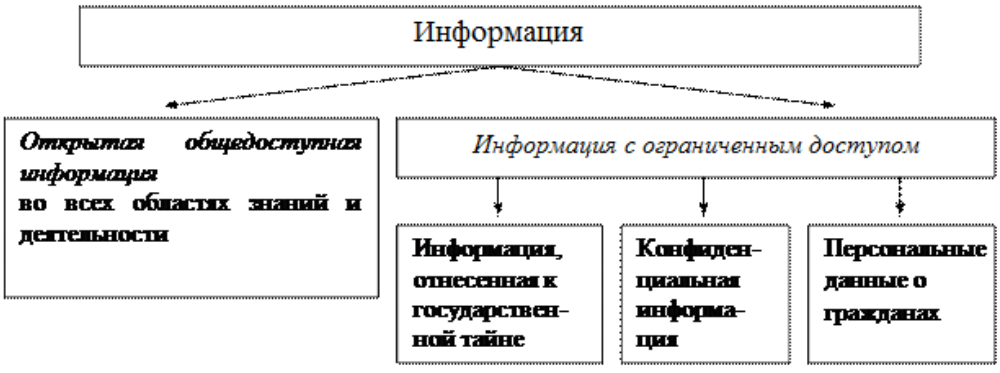


Рис. 1. Категории информации в зависимости от категории доступа к ней

Из *Закона об информации* следует, что:

· к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен;

· категория «информация с ограниченным доступом» объединяет все виды защищаемой информации: персональные данные о гражданах, конфиденциальная информация (все виды тайн: коммерческая, служебная, профессиональная и иная), при этом, исключение составляет информация, отнесённая к *государственной тайне* - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. Такая информация к конфиденциальной не относится, а является составной частью информации с ограниченным доступом.

Обладатель информации (т.е. лицо, самостоятельно создавшее информацию, либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам), *оператор информационной системы* (т.е. гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных) в случаях, установленных законодательством РФ, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Целостность информации - свойство сохранять свою структуру и содержание в процессе хранения, использования и передачи.

Достоверность информации - свойство, выражаемое в строгой принадлежности информации субъекту, который является ее источником.

Под *доступом к информации* понимается возможность получения информации и её использования.

Санкционированный доступ к информации - доступ с выполнением правил разграничения доступа к информации.

Несанкционированный доступ - чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий.

Правила разграничения доступа - регламентация прав доступа субъекта к определенному компоненту системы.

Идентификация - получение от субъекта доступа сведений (имя, учетный номер и т.д.), позволяющих выделить его из множества субъектов.

Аутентификация - получение от субъекта сведений (пароль, биометрические параметры и т.д.), подтверждающих, что идентифицируемый субъект является тем, за кого себя выдает.

Термин **информационная безопасность** в разных контекстах может иметь различное значение.

В Доктрине информационной безопасности РФ он используется в широком смысле и означает состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В рамках изучаемой дисциплины основное внимание уделяется информационным процессам хранения, обработки и передачи информации вне зависимости от того, на каком языке она закоди-

рована, кто или что является ее источником, и какое психологическое воздействие на человека она оказывает. Поэтому в данной дисциплине термин информационная безопасность будет рассматриваться в узком смысле и означать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Следовательно, угроза информационной безопасности – это оборотная сторона использования информационных технологий. Из этого положением можно вывести два важных следствия:

1. Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно отличаться.
2. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие (например: поломка системы, приведшая к перерыву в работе).

К поддерживающей инфраструктуре следует отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций, а также обслуживающий персонал.

Информационная безопасность – многогранная, многомерная область деятельности, в которой успех может принести только системный, комплексный подход. Спектр интересов субъектов, связанных с использование информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

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

Целостность – это актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. То есть целостность предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. Целостность можно подразделить на статическую (неизменность информационных объектов) и динамическую (корректное выполнение сложных действий – транзакций). Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например, техническими, социальными 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.

Конфиденциальность – это защита от несанкционированного доступа к информации. Основным средством обеспечения конфиденциальности является шифрование информации. Конфиденциальная информация 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 – самый проработанный у нас в стране аспект информационной безопасности.

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

С позиций системного подхода к защите информации предъявляются определенные требования. Защита информации должна быть:

- Непрерывной.
- Плановой. Каждая служба разрабатывает план защиты информации в сфере своей компетенции.
- Целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели.
- Конкретной. Защищаются конкретные данные, объективно подлежащие защите.
- Активной.
- Надежной.
- Универсальной. Распространяется на любые каналы утечки информации.
- Комплексной. Применяются все необходимые виды и формы защиты.

К системе безопасности информации предъявляются следующие требования:

- четкость определения полномочий и прав пользователей на доступ к определенным видам информации;
- предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;
- сведение к минимуму числа общих для нескольких пользователей средств защиты;
- учет случаев и попыток несанкционированного доступа к конфиденциальной информации;
- обеспечение оценки степени конфиденциальной информации;
- обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя

Система защиты информации (СЗИ), как и любая система, должна иметь определенные виды собственного обеспечения (совокупность обеспечивающих подсистем), опираясь на которые она будет выполнять свою целевую функцию. В частности, СЗИ может иметь:

1. **Правовое обеспечение**. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия.
2. **Организационное обеспечение**. Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами, такими как: служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая служба и другими.
3. **Аппаратное обеспечение**. Предполагается широкое использование технических средств, как для защиты информации, так и для обеспечения деятельности самой СЗИ.
4. **Информационное обеспечение**. Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности.
5. **Программное обеспечение**. К нему относятся различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей несанкционированного проникновения к источникам конфиденциальной информации.
6. **Математическое обеспечение**. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты.
7. **Лингвистическое обеспечение**. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации.
8. **Нормативно-методическое обеспечение**. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации.

Под системой безопасности будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз. Как и любая система, система информационной безопасности имеет свои цели, задачи, методы и средства деятельности, которые согласовываются по месту и времени в зависимости от условий. На рисунке 2 представлена концептуальная модель безопасности информации.

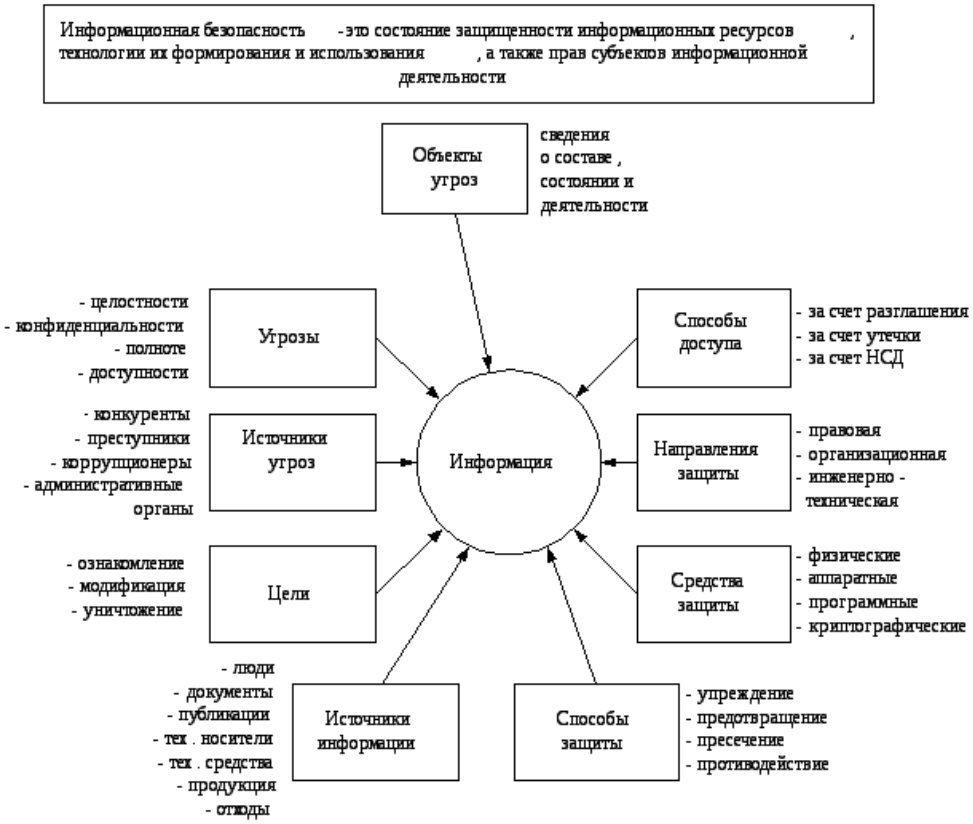


Рис.2. Концептуальная модель безопасности информации

В каждой организации разрабатывается концепция информационной безопасности. Она является основным правовым документом, определяющим защищенность предприятия от внутренних и внешних угроз. Она определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в ИС. Концепция является методологической основой:

- формирования и проведения единой политики в области обеспечения безопасности информации в ИС;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
- координации деятельности структурных подразделений при проведении работ по созданию, развитию и эксплуатации ИС с соблюдением требований обеспечения безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ИС.

При разработке концепции должны учитываться основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно- программных средств защиты и противодействия угрозам безопасности информации, а также текущее состояние и перспективы развития информационных технологий.

Основные положения концепции должны базироваться на качественном осмыслении вопросов безопасности информации и не концентрировать внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

Положения концепции предусматривают существование в рамках проблемы обеспечения безопасности информации в ИС двух относительно самостоятельных направлений, объединенных единым замыслом: защита информации от утечки по техническим каналам и защита информации в ИС от несанкционированного доступа.

В организации, как правило, подразделение, занимающееся защитой информации, называется **службой информационной безопасности**. Зачастую это лишь несколько сотрудников. Структура органов (подразделения) должна:

- руководствоваться нормативной БАЗОЙ, где описаны ее состав, назначение и функции;
- действовать в соответствии с установленными МЕРАМИ, т.е. выполнять принятую в организации политику информационной безопасности;
- иметь в своем распоряжении соответствующие СРЕДСТВА, т.е. техническое оснащение.

При этом СТРУКТУРА должна решать задачи обеспечения безопасности информации по ЭТАПАМ, на соответствующих НАПРАВЛЕНИЯХ.

БАЗА. Разумеется, основные положения политики безопасности должны быть закреплены в соответствующих распорядительных документах, состав и содержание которых определяются спецификой объекта защиты. Однако, как правило, ни одна организация не может обойтись без положений о коммерческой тайне, о защите информации, об администраторе безопасности сети, о разграничении прав доступа к информации.

МЕРЫ. Основу политики безопасности составляет перечень обязательных мероприятий, направленных на выработку плана действий по информационной защите объекта: определение состава службы по защите информации, ее место в организационной структуре предприятия, сфера ее компетенции, права и полномочия, варианты действий в различных ситуациях во избежание конфликтов между подразделениями.

Работы по обеспечению функционирования службы ЗИ входят в комплекс организационных мер, на основе которых может быть достигнут высокий уровень безопасности информации. Тем не менее, перечисленные меры не позволят на должном уровне поддерживать функционирование системы защиты без целого ряда организационно-технических мероприятий. Их проведение позволяет своевременно выявлять новые каналы утечки информации, принимать меры по их нейтрализации, совершенствованию системы защиты и оперативно реагировать на нарушения режима безопасности.

СРЕДСТВА. Использование качественных средств защиты позволяет закрывать большинство уязвимых мест, если информация о «дырах» в системах безопасности обновляется достаточно оперативно – по мере их нахождения специальными группами экспертов в области информационной безопасности.

Правильно отработанная методика проведения работ по ЗИ гарантирует, что ни один аспект информационной безопасности не останется без внимания.

ЭТАПЫ:

- Определение информации, подлежащей защите
- Выявление угроз и каналов утечки информации
- Проведение оценки уязвимости и рисков
- Определение требований к системе ЗИ
- Осуществление выбора средств защиты
- Внедрение и использование выбранных мер и средств

• Контроль целостности и управление защитой.

НАПРАВЛЕНИЯ:

• Защита объектов информационной системы
• Защита процессов и программ
• Защита каналов связи
• ПЭМИН
• Управление системой защиты.

Перечень задач, решаемых службой информационной безопасности.

1. Определение информационных и технических ресурсов, подлежащих защите. Для решения этой задачи необходимо рассмотреть функции органов (лиц), ответственных за определение информации (сведений) и средств, подлежащих защите на различных НАПРАВЛЕНИЯХ. К сожалению, часто бывает так, что меры безопасности информации становятся и мерами распределения потоков информации. Это может привести к довольно громоздким процедурам и вызвать впечатление у сотрудников, что меры безопасности усложняют их работу.

Если придется создавать систему безопасности информации, рекомендуется сначала присмотреться к процедурам распределения информации в этой организации.

2. Выявление полного множества потенциально возможных угроз и каналов утечки информации. Процедуры безопасности могут обеспечить проверку паролей и строгий контроль доступа к ценным общим данным, но взломщика, хорошо знающего внутреннее устройство системы, практически невозможно остановить. Одной из наиболее уязвимых точек любой организации с точки зрения безопасности становится ее персонал, и, соответственно, большое значение приобретают грамотная реализация внутренней политики и работа с персоналом, которая предусматривает:

• подбор и расстановку кадров;
• адаптирование сотрудника к новому коллективу;
• распределение задач и ответственности;
• обучение и повышение квалификации;
• мотивацию поведения сотрудников;
• контроль за исполнением сотрудником возложенных на него функций;
• мониторинг психологического климата в коллективе;
• выявление неудовлетворенных своим положением и нелояльных сотрудников;
• увольнение сотрудников.

Среди указанных видов работ в компетенцию службы ИБ организации входит выявление нелояльных сотрудников (сотрудников, которые работают на конкурента) и сотрудников, не удовлетворенных своим положением в коллективе и, поэтому потенциально готовых работать на конкурента.

3. Проведение оценки уязвимости и рисков для информации и ресурсов информационной системы. Для построения надежной защиты необходимо выявить возможные угрозы безопасности информации, оценить их последствия, определить необходимые меры и средства защиты и оценить их эффективность. Поскольку анализ всей информационной инфраструктуры (особенно для крупных объектов) далеко не всегда оправдан с экономической точки зрения, иногда бывает целесообразно сосредоточиться на наиболее важных объектах, отдавая себе отчет в приближенности итоговой оценки. С этих же позиций следует оценивать возможные угрозы и их последствия.

Разнообразие потенциальных угроз столь велико, что не позволяет предусмотреть каждую из них, поэтому анализируемые виды следует выбирать с позиций здравого смысла, одновременно выявляя не только угрозы, вероятность их осуществления, размер потенциального ущерба, но и их источники.

Оценка рисков производится с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации. На основании результатов анализа выявляются наиболее высокие риски, переводящие потенциальную угрозу в разряд реально опасных и,

следовательно, требующие принятия дополнительных защитных мер. Как правило, для каждой подобной угрозы существует несколько вариантов решения по ее нейтрализации.

4. Определение требований к системе ЗИ.

Строится функциональная схема системы ЗИ. СхФ + Политика безопасности + Ответственность персонала + Порядок ввода в действие средств защиты + План размещения средств защиты и их модернизации = План защиты.

5. Осуществление выбора средств ЗИ и их характеристик. Решение организационных вопросов предваряет этап работ, который должен ответить на вопрос: что необходимо сделать для реализации выбранной политики безопасности?

6. Внедрение и организация использования выбранных мер, способов и средств защиты.

Требуется организационно-техническая и организационно-правовая поддержка.

7. Осуществление контроля целостности и управление системой защиты.

Ежегодный пересмотр Плана защиты. Проверка, тестирование программно-технических средств.

Социальная инженерия и её методы

Методы манипулирования человеком известны достаточно давно, в основном они пришли в социальную инженерию из арсенала различных спецслужб.

Первый известный случай конкурентной разведки относится к VI веку до нашей эры и произошёл в Китае, когда китайцы лишились секрета изготовления шелка, который обманным путём выкрали римские шпионы.

Социальная инженерия — наука, которая определяется как набор методов манипулирования поведением человека, основанных на использовании слабостей человеческого фактора, без применения технических средств.

По мнению многих специалистов, самую большую угрозу ИБ представляют именно методы социальной инженерии, хотя бы потому, что использование социального хакерства не требует значительных финансовых вложений и доскональных знаний компьютерных технологий, а также потому, что людям присущи некоторые поведенческие наклонности, которые можно использовать для осторожного манипулирования.

И как бы не совершенствовались технические системы защиты, люди так и будут оставаться людьми со своими слабостями, предрассудками, стереотипами, с помощью которых и происходит управление. Настроить же человеческую «программу безопасности» — самое сложное и не всегда приводящее к гарантированным результатам дело, так как этот фильтр необходимо подстраивать постоянно. Здесь как никогда актуально звучит главный девиз всех экспертов по безопасности: «Безопасность — это процесс, а не результат»

Области применения социальной инженерии:

1.общая дестабилизация работы организации с целью снижения её влияния и возможности последующего полного разрушения организации;

2.финансовые махинации в организациях;

3.фишинг и другие способы кражи паролей с целью доступа к персональным банковским данным частных лиц;

4.воровство клиентских баз данных;

5.конкурентная разведка;

6.общая информация об организации, о её сильных и слабых сторонах, с целью последующего уничтожения данной организации тем или инным способом (часто применяется для рейдерских атак);

7.информация о наиболее перспективных сотрудниках с целью их дальнейшего «переманивания» в свою организацию;

Социальное программирование и социальное хакерство

Методы социального программирования привлекательны тем, что о них либо вообще никто никогда не узнает, либо даже если кто-то о чем-то догадывается, привлечь к ответственности такого деятеля очень сложно, а также в ряде случаев можно «программировать» поведение людей,

причем и одного человека, и большой группы. Данные возможности относятся к категории социального хакерства именно по той причине, что во всех из них люди выполняют чью-то чужую волю, как бы подчиняясь написанной социальным хакером «программе».

Социальное хакерство как возможность взлома человека и программирования его на совершение нужных действий исходит из социального программирования — прикладной дисциплины социальной инженерии, где специалисты этой сферы — социальные хакеры — используют приёмы психологического воздействия и актёрского мастерства, заимствованные из арсенала спецслужб.

Социальное хакерство применяется в большинстве случаев тогда, когда речь идёт об атаке на человека, который является частью компьютерной системы. Компьютерная система, которую взламывают, не существует сама по себе. Она содержит важную составляющую — человека. И чтобы получить информацию, социальному хакеру необходимо взломать человека, который работает с компьютером. В большинстве случаев проще сделать это, чем взломать компьютер жертвы, пытаясь таким образом узнать пароль.

Типовой алгоритм воздействия в социальном хакерстве:

Все атаки социальных хакеров укладывается в одну достаточно простую схему:

1.формулируется цель воздействия на тот или другой объект;

2.собирается информация об объекте, с целью обнаружения наиболее удобных мишеней воздействия;

3.на основе собранной информации реализуется этап, который психологи называют аттракцией. Аттракция (от лат. Attrahere – привлекать, притягивать) — это создание нужных условий для воздействия на объект;

4.принуждение к нужному для социального хакера действию;

Принуждение достигается выполнением предыдущих этапов, т. е. после того, как достигнута аттракция, жертва сама делает нужные социоинженеру действия.

На основании собранной информации социальные хакеры достаточно точно прогнозируют психо- и социотип жертвы, выявляя не только потребности, в еде, сексе и прочее, но и потребность в любви, потребность в деньгах, потребность в комфорте и т. д и т. п.

И действительно, зачем пытаться проникать в ту или другую компанию, взламывать компьютеры, банкоматы, организовывать сложные комбинации, когда можно сделать все легче: влюбить в себя до беспамятства человека, который по своей доброй воле будет переводить деньги на указанный счет или каждый раз делиться необходимой информацией?

Основываясь на том, что поступки людей предсказуемы, а также подчиняются определенным законам, социальные хакеры и социальные программисты для выполнения поставленных задач используют как оригинальные многоходовки, так и простые положительные и отрицательные приемы, основанные на психологии человеческого сознания, программах поведения, колебаниях внутренних органов, логическом мышлении, воображении, памяти, внимании. К этим приёмам можно отнести:

генератор Вуда — генерирует колебания той же частоты, что и частота колебаний внутренних органов, после чего наблюдается эффект резонанса, в результате которого люди начинают ощущать сильный дискомфорт и паническое состояние;

воздействие на географию толпы — для мирного расформирования крайне опасных агрессивных, больших групп людей;

высоко частотные и низкочастотные звуки — для провоцирования паники и её обратного эффекта, а также других манипуляций;

программа социального подражания — человек определяет правильность поступков, выясняя, какие поступки считают правильными другие люди;

программа клакерства — (на основе социального подражания) организация необходимой реакции зрителей;

формирование очередей — (на основе социального подражания) простой, но действенный рекламный ход;

программа действия авторитета — беспрекословное исполнение приказов человека, являющегося авторитетом;

программа взаимопомощи — человек стремится отплатить добром тем людям, которые ему сделали какое-то добро. Стремление выполнить эту программу зачастую превышает все доводы рассудка;

а также интернет рекламу и антирекламу, распространение слухов и т.д. и т. п.

Социальное хакерство в интернете

С появлением и развитием Интернета — виртуальной среды, состоящей из людей и и их взаимодействий, расширилась среда для манипулирования человеком, для получения нужной информации и совершения необходимых действий. В наши дни Интернет является средством общемирового вещания, средой для сотрудничества, общения и охватывает весь земной шар. Именно этим и пользуются социальные инженеры для достижения своих целей.

Способы манипулирование человеком через Интернет:

В современном мире владельцы практически каждой компании уже осознали, что интернет – это очень эффективное и удобное средство для расширения бизнеса и основная его задача – это увеличение прибыли всей компании. Известно, что без информации направленной на привлечение внимания, к нужному объекту, формирования или поддержание интереса к нему и его продвижение на рынке используется реклама. Только, в связи с тем, что рекламный рынок уже давно поделен, большинство видов рекламы для большинства предпринимателей, впустую потраченные деньги. Интернет реклама это не просто одна из разновидностей рекламы в СМИ, это нечто большее, поскольку с помощью интернет рекламы на сайт организации приходят люди, заинтересованные в сотрудничестве.

Интернет реклама, в отличие от рекламы в СМИ, имеет намного больше возможностей и параметров управления рекламной компанией. Наиболее важным показателем Интернет рекламы является то, что плата за Интернет рекламу списывается только при переходе заинтересовавшегося пользователя по ссылке рекламы, что конечно делает рекламу в Интернете более эффективной и менее затратной чем реклама в СМИ. Так подав рекламу на телевидении или в печатных изданиях, её оплачивают полностью и просто ждут потенциальных клиентов, но клиенты могут откликнуться на рекламу или нет — все зависит от качества изготовления и подачи рекламы на телевидении или газетах, однако бюджет на рекламу уже израсходован и в случае если реклама не по действовала — израсходован впустую. В отличие от такой рекламы в СМИ, реклама в Интернете имеет возможности отслеживания отклика аудитории и управления Интернет рекламой до того как ее бюджет израсходован, более того, рекламу в Интернете можно приостановить — когда спрос на продукцию возрос и возобновить — когда спрос начинает падать.

Другим способом воздействия является так называемое «Убийство форумов» где, с помощью социального программирования создают антирекламу тому или иному проекту. Социальный программист в данном случае, с помощью явных провокаторских действий в одиночку, разрушает форум, пользуясь при этом несколькими псевдонимами (*nickname*) для создания вокруг себя антилидерской группировки, и привлечения в нее постоянных посетителей проекта, недовольных поведением администрации. В конце подобных мероприятий не форуме становится невозможным проджинение товаров или идей. Для чего первоначально и разрабатывался форум.

К способам воздействия на человека через интернет в целях социальной инженерии:

Фишинг — вид интернет-мошенничества, с целью получение доступа к конфиденциальным данным пользователей — логинам и паролям. Данная операция достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов (Rambler), банков или внутри социальных сетей (Facebook). В письме часто содержится ссылка на сайт, внешне неотличимый от настоящего. После того, как пользователь попадает на поддельную страницу, социальные инженеры различными приёмами побуждают пользователя ввести на странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет получить доступ к аккаунтам и банковским счетам.

Более опасным видом мошенничества, чем фишинг, является так называемый фарминг.

Фарминг — механизм скрытого перенаправления пользователей на фишинговые сайты. Социальный инженер распространяет на компьютеры пользователей специальные вредоносные программы, которые после запуска на компьютере перенаправляют обращения с необходимых сайтов на поддельные. Таким образом, обеспечивается высокая скрытность атаки, а участие пользователя сведено к минимуму – достаточно дождаться, когда пользователь решит посетить интересующие социального инженера сайты.

Потенциальные угрозы безопасности информации

Угроза информационной безопасности – это потенциальная возможность нарушения режима ИБ. Преднамеренная реализация угрозы называется **атакой** на автоматизированную систему. Лица, преднамеренно реализующие угрозы, являются **злоумышленниками**. Потенциальные злоумышленники называются источниками угрозы.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем, например, неконтролируемый доступ к персональным компьютерам или нелицензионное программное обеспечение (к сожалению даже лицензионное программное обеспечение не лишено уязвимостей).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на АС.

Если речь идет об ошибках в ПО, то окно опасности "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих. Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

должно стать известно о средствах использования пробела в защите;

должны быть выпущены соответствующие заплаты;

заплаты должны быть установлены в защищаемой АС.

Само понятие "угроза" в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать -вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью.

Отметим, что некоторые угрозы нельзя считать следствием целенаправленных действий вредного характера. Существуют угрозы, вызванные случайными ошибками или техногенными явлениями.

Знание возможных угроз информационной безопасности, а также уязвимых мест системы защиты, необходимо для того, чтобы выбрать наиболее экономичные и эффективные средства обеспечения безопасности. Слишком много мифов существует в сфере информационных технологий (вспомним все ту же "Проблему 2000"), поэтому незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

Угрозы ИБ классифицируются по нескольким признакам:

- **по составляющим информационной безопасности** (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;
- **по компонентам информационных систем**, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- **по характеру воздействия** (случайные или преднамеренные, действия природного или техногенного характера);
- **по расположению источника угроз** (внутри или вне рассматриваемой информационной системы).

Отправной точкой при анализе угроз информационной безопасности является определение составляющей информационной безопасности, которая может быть нарушена той или иной угрозой: конфиденциальность, целостность или доступность.

Рассмотрим угрозы **по характеру воздействия**.

Опыт проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы.

Причинами *случайных воздействий* при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия злоумышленника. В качестве злоумышленника могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами, например:

- недовольством служащего служебным положением;
- любопытством;
- конкурентной борьбой;
- уязвленным самолюбием и т. д.

Угрозы, классифицируемые **по расположению источника угроз**, бывают внутренние и внешние.

Внешние угрозы обусловлены применением вычислительных сетей и создание на их основе информационных систем.

Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно

Новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат - как можно более оперативно.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные АС.

В качестве основного критерия мы будем использовать по аспекту ИБ, привлекая при необходимости остальные наиболее распространенные угрозы доступности.

Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки и являются собственно угрозами (неправильно веденные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь - следствие непреднамеренных ошибок.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

отказ пользователей;

внутренний отказ информационной системы;

отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующую угрозу:

нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);

невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение работать с документацией и т.п.):

невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

нарушение работы (случайное или умышленное) систем сети, электропитания, водо- и/или теплоснабжения, кондиционирования:

разрушение или повреждение помещений;

невозможность или нежелание обслуживающего персонала и пользователей выполнять свои обязанности (аварии на транспорте, террористический акт, забастовка и т.п.).

Весьма опасны так называемые "обиженные" сотрудники — нынешние и бывшие. Как правило, они стремятся нанести вред организации-"обидчику", например:

испортить оборудование;

встроить логическую бомбу, которая со временем разрушит программы и/или данные;

удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Угрозы доступности могут выглядеть грубо — как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранят небрежно, не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме — как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание.

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок.

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения. Выделим следующие грани вредоносного ПО:

вредоносная функция;

способ распространения;

внешнее представление.

По механизму распространения различают:

вирусы — код, обладающий способностью к распространении (возможно, с изменениями) путем внедрения в другие программы;

"черви" — код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. "Черви", напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Для внедрения "бомб" часто используются ошибки типа "переполнение буфера", когда программа, работая с областью памяти, выходит за границы допустимого и записывает в нужные злоумышленнику места определенные данные.

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты.

С целью нарушения статической целостности злоумышленник может: ввести неверные данные; изменить данные.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение вредоносного ПО пример подобного нарушения.

Основные угрозы целостности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Ранее мы проводили различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

ввести неверные данные;

изменить данные.

Иногда изменяются содержательные данные, иногда - служебная информация.

Еще один урок: угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить "неотказуемость", компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Основные угрозы конфиденциальности

Перехват данных — очень серьезная утром, и если конфиденциальность действительно является критичной, а данные пересылаются но многим каналам, их зашита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например па кабельную сеть, может кто угодно, так что эту угрозу нужно принимать, во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

К неприятным угрозам, от которых трудно защищаться, можно отнести и злоупотребление полномочиями. Таковы основные угрозы, которые наносит наибольший ущерб субъектам информационных отношений.

Каждая угроза влечет за собой **определенный ущерб** (потери) — моральные или материальные, а меры по противодействию этой угрозе призваны снизить ее величину до приемлемого уровня.

Оценка возможных ущербов (потерь) предполагает знание видов потерь, связанных с предпринимательской деятельностью, и умение вычисления их вероятностной прогнозной величины. Существуют следующие виды возможных ущербов (потерь):

1. **Материальные виды потерь** проявляются в непредусмотренных предпринимательским проектом дополнительных затратах или прямых потерях оборудования, имущества, продукции, сырья, энергии и т. д.

2. **Трудовые потери** — это потери рабочего времени, вызванные случайными, непредвиденными обстоятельствами; измеряются в часах рабочего времени. Перевод трудовых потерь в де-

нежное выражение осуществляется путем умножения трудочасов на стоимость (цену) одного часа.

3. **Кадровые потери** — потери необходимых предприятию профессиональных, высококвалифицированных работников; измеряются в затратах на подбор и обучение нового кадрового состава в денежном выражении.

4. **Финансовые потери** — прямой денежный ущерб, связанный с непредусмотренными платежами, выплатой штрафов, уплатой дополнительных налогов, потерей денежных средств и ценных бумаг.

5. **Временные потери**. Происходят, когда процесс предпринимательской деятельности идет медленнее, чем намечено. Прямая оценка таких потерь осуществляется в часах, днях, неделях, месяцах запаздывания в получении намеченного результата. Чтобы перевести оценку потерь времени в денежное измерение, необходимо установить, к каким потерям дохода, прибыли способны приводить потери времени. В конечном итоге оцениваются в денежном выражении.

6. **Информационные потери**. Одни из самых серьезных потерь в бизнесе, способные привести к краху всей организации. Исчисляются в стоимостном выражении.

7. **Особые виды потерь** проявляются в виде нанесения ущерба здоровью и жизни людей, окружающей среде, престижу предпринимателя, а также вследствие других неблагоприятных социальных и морально - психологических последствий.

Информационный ущерб (потери) связан с наличием в процессе предпринимательской деятельности информационного риска, который входит в общий предпринимательский риск.

Информационный риск - вероятность (угроза) потерь активов субъекта экономики (предпринимателя) в результате потерь, порчи, искажения и разглашения информации.

Информационный риск классифицируется следующим образом:

– риск прерывания информации (прекращение нормальной обработки информации, например, вследствие разрушения, вывода из строя вычислительных средств). Такая категория действий может вызвать весьма серьезные последствия, если даже информация при этом не подвергается никаким воздействиям;

– риск кражи информации (считывание или копирование информации, хищение носителей информации и результатов печати с целью получения данных, которые могут быть использованы против интересов владельца (собственника) информации);

– риск модификация информации (внесение несанкционированных изменений в данные, направленных на причинение ущерба владельцу (собственнику) информации);

– риск разрушения данных (необратимое изменение информации, приводящее к невозможности ее использования);

– риск электромагнитного воздействия и перехвата информации в автоматизированных и информационных системах (АИС);

– риск съема информации по акустическому каналу;

– риск прекращения питания АИС и поддерживающей инфраструктуры);

– риск ошибки операторов и поставщиков информационных ресурсов АИС;

– риск сбоев программного обеспечения АИС;

– риск неисправности аппаратных устройств АИС (в результате халатных действий сотрудников, несоблюдения техники безопасности, природных катаклизмов, сбоев программных средств и т. д.).

В конечном итоге все противоправные действия приводят к нарушению конфиденциальности, целостности и доступности информации.

Таким образом, перечень угроз и источников их возникновения достаточно разнообразен и предложенная классификация не является исчерпывающей. Противодействие проявлениям угроз осуществляется по различным направлениям, с использованием полного арсенала методов и средств защиты.

Угрозы промышленного шпионажа и основные способы его ведения

Одной из самых серьезных угроз коммерческой деятельности является промышленный шпионаж. **Сущность промышленного шпионажа** - стремление к овладению конфиденциальной информацией конкурентов с целью получения максимальной коммерческой выгоды. Он заключается в получении любой информации о новейших научно-технических разработках, коммерческих планах, состоянии дел и т. п. Ведется всеми доступными средствами, включая применение специальных технических средств и подкуп должностных лиц.

Сбор сведений ведется самыми различными способами, но при этом основными каналами утечки информации являются:

открытые источники;

субъекты - носители информации;

технические средства разведки.

К **открытым источникам** относятся каналы, по которым информацию можно почерпнуть без нарушения каких-либо ограничений или запретов: например, из газет, книг, научных и технических изданий, официальных отчетов и особенно - рекламных каталогов и брошюр. Главными объектами такого анализа получения конфиденциальной информации являются: доклады на конференциях, симпозиумах и т. д.; попытки пригласить на работу сотрудников конкурирующей организации и заполнение ими при этом специальных вопросников; прием на работу, с увеличением оклада, служащего конкурирующей организации (законный подкуп); изучение выставочных образцов; притворные переговоры с конкурентами и т. д.

Использование субъектов – наиболее распространенный метод промышленного шпионажа. При определенных условиях люди способны скрывать, воровать, продавать информацию и совершать иные криминальные действия вплоть до вступления в устойчивые преступные связи со злоумышленниками. Основными вариантами использования субъектов – физических лиц, являются следующие: Засланный агент. Внедренный агент. Нарушитель. Агент - постоянный посетитель в местах общего пользования служащих. Агент слежки. «Сборщик мусора». Организатор опроса общественного мнения. Агент, обращающийся к руководству с заманчивыми предложениями. Инженер, анализирующий чужую продукцию, выявляющий секреты производства или процесса. Вербовщик посетителей, с целью их использования в качестве агентуры на выбранном для шпионажа объекте.

Технические средства промышленного шпионажа применяются в случае невозможности использования агентурных средств.

Общая характеристика основных методов получения информации о различных сторонах деятельности и перечень используемых при этом технических средств приведены в таблице.

№	Действия	Физическое явление	Способ (средство) съема информации
1	Разговор нескольких лиц	Акустический сигнал	Подслушивание, в том числе случайное. Диктофоны. Закладные устройства с передачей информации по: имеющимся коммуникациям (трубам, цепям сигнализации, сетям 220 В, телефонным линиям...); специально проложенным проводам; радио- или ИК-каналу Направленные микрофоны
		Виброакустический сигнал	Стетоскоп. Вибродатчик с передачей информации по: радиоканалу; проводам; коммуникациям; ИК-каналу Оптический лазерный микрофон
		Гидроакустический сигнал	Гидроакустический датчик
		Акустоэлектрический сигнал	Радиоприемник спецназначения
		Движение губ	Визуально, в том числе оптическими приборами Камера, в том числе с передачей по проводам и радиоканалу
2	Разговор по телефону.	Акустический сигнал	Аналогично п. 1

		Электрический сигнал в линии	Параллельный телефон, прямое подключение, подключение через электромагнитный датчик, телефонная радиозакладка
		Побочные электромагнитные излучения и наводки	Специальные радиотехнические устройства
3	Разговор по радиотелефону	Акустический сигнал Электромагнитные волны	Аппаратура п. 1 Специальные радиоприемные устройства
4	Документ на бумажном носителе	Наличие	Визуально, в том числе с помощью оптических средств Фотографирование, в том числе с дистанционной передачей снимка Копирование
5	Размножение документа на бумажном носителе	Печать документа на принтере	Кража, визуально
		Шумы принтера	Спецаппаратура акустического контроля
		ПЭМИ от ЭВМ	Специальные радиотехнические устройства
6	Почтовые отправления	Наличие	Прочтение: со вскрытием, без вскрытия
7	Документ на небумажном носителе	Носитель	Копирование, вскрытие, несанкционированное использование ЭВМ
8	Изготовление документа на небумажном носителе	Изображение на дисплее	Визуально, в том числе с помощью оптических средств Фотографирование. Видео- или телевизионные закладные устройства
		ПЭМИ	Специальные радиотехнические устройства
		Электрические сигналы в сетях	Аппаратные закладки
9	Передача документа на небумажном носителе	Электрические сигналы	Несанкционированное подключение, имитация пользователя

Вредоносное программное обеспечение. Компьютерные вирусы и средства защиты от них.

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения. Мы выделим следующие грани вредоносного ПО:

вредоносная функция;

способ распространения;

внешнее представление.

Часть, осуществляющую разрушительную функцию, будем называть "бомбой" (хотя, возможно, более удачными терминами были бы "заряд" или "боеголовка"). Вообще говоря, спектр вредоносных функций неограничен, поскольку "бомба", как и любая другая программа, может обладать сколь угодно сложной логикой, но обычно "бомбы" предназначаются для:

внедрения другого вредоносного ПО;

получения контроля над атакуемой системой;

агрессивного потребления ресурсов;

изменения или разрушения программ и/или данных.

По механизму распространения различают:

вирусы - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

"черви" - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Отметим, что данные нами определения и приведенная классификация вредоносного ПО отличаются от общепринятых. Например, в ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения" содержится следующее определение:

"Программный вирус - это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах".

На наш взгляд, подобное определение неудачно, поскольку в нем смешаны функциональные и транспортные аспекты. Окно опасности для вредоносного ПО появляется с выпуском новой разновидности "бомб", вирусов и/или "червей" и перестает существовать с обновлением базы данных антивирусных программ и наложением других необходимых заплат.

По традиции из всего вредоносного ПО наибольшее внимание общественности приходится на долю вирусов. Однако до марта 1999 года с полным правом можно было утверждать, что "несмотря на экспоненциальный рост числа известных вирусов, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. Соблюдение несложных правил "компьютерной гигиены" практически сводит риск заражения к нулю. Там, где работают, а не играют, число зараженных компьютеров составляет лишь доли процента".

В марте 1999 года, с появлением вируса "Melissa", ситуация кардинальным образом изменилась. "Melissa" - это макровирус для файлов MS-Word, распространяющийся посредством электронной почты в присоединенных файлах. Когда такой (зараженный) присоединенный файл открывают, он рассылает свои копии по первым 50 адресам из адресной книги Microsoft Outlook. В результате почтовые серверы подвергаются атаке на доступность.

Действие вредоносного ПО может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности.

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. "Черви", напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, "черви" "съедают" полосу пропускания сети и ресурсы почтовых систем. По этой причине для атак на доступность они не нуждаются во встраивании специальных "бомб".

Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Компьютерный вирус – специально написанная программа, способная самопроизвольно присоединиться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе на компьютере.

Проникнув в один компьютер, вирус способен распространиться на другие.

Основными типами компьютерных вирусов являются:

• программные вирусы;

• загрузочные вирусы;

• макровирусы.

К компьютерным вирусам примыкают и так называемые троянские кони (троянские программы).

Программные вирусы —это блоки программного кода, целенаправленно внедренные внутрь других прикладных программ. При запуске программы, несущей вирус, происходит запуск имплантированного в нее вирусного кода.

Работа этого кода вызывает скрытые от пользователя изменения в файловой системе жестких дисков и/или в содержании других программ. Так, например, вирусный код может воспроизводить себя в теле других программ — этот процесс называется размножением. По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к раз-

рушительным действиям — нарушению работы программ и операционной системы, удалению информации, хранящейся на жестком диске. Этот процесс называется вирусной атакой.

Самые разрушительные вирусы могут инициировать форматирование жестких дисков. Поскольку форматирование диска — достаточно продолжительный процесс, который не должен пройти незамеченным со стороны пользователя, во многих случаях программные вирусы ограничиваются уничтожением данных только в системных секторах жесткого диска, что эквивалентно потере таблиц файловой структуры. В этом случае данные на жестком диске остаются нетронутыми, но воспользоваться ими без применения специальных средств нельзя, поскольку неизвестно, какие сектора диска каким файлам принадлежит.

Теоретически восстановить данные в этом случае можно, но трудоемкость этих работ исключительно высока. Т.к. аппаратное и программное обеспечение настолько взаимосвязаны, бывают случаи, что программные повреждения приходится устранять заменой аппаратных средств.

Программные вирусы поступают на компьютер при запуске непроверенных программ, полученных на внешнем носителе или принятых из Интернета. При обычном копировании зараженных файлов заражение компьютера произойти не может. В связи с этим все данные, принятые из Интернета, должны проходить обязательную проверку на безопасность, а если получены незатребованные данные из незнакомого источника, их следует уничтожать, не рассматривая.

Обычный прием распространения «троянских» программ — приложение к электронному письму с «рекомендацией» извлечь и запустить якобы полезную программу.

Загрузочные вирусы. От программных вирусов загрузочные вирусы отличаются методом распространения. Они поражают не программные файлы, а определенные системные области магнитных носителей. Кроме того, на включенном компьютере они могут временно располагаться в оперативной памяти. Обычно заражение происходит при попытке загрузки компьютера с магнитного носителя, системная область которого содержит загрузочный вирус. Происходит сначала проникновение вируса в оперативную память, а затем в загрузочный сектор жестких дисков. Далее этот компьютер сам становится источником распространения загрузочного вируса.

Макровирусы. Эта особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых 4 макрокоманд. В частности, к таким документам относятся документы текстового процессора Microsoft Word (они имеют расширение .DOC). Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд. Как и для других типов вирусов, результат атаки может быть как относительно безобидным, так и разрушительным.

Вирусы так же можно разделить на классы по следующим признакам:

· по среде обитания вируса;

· по способу заражения;

· по деструктивным возможностям

· по особенностям алгоритма вируса

По среде обитания вирусы можно разделить на:

сетевые,

файловые (программные),

загрузочные.

Сетевые вирусы распространяются по компьютерной сети, файловые внедряются в выполняемые файлы (программы), загрузочные - в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record).

Существуют сочетания - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы и часто применяют оригинальные методы проникновения в систему.

По способу заражения вирусы делятся на резидентные и нерезидентные.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам

заражения 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. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными.

По деструктивным возможностям вирусы можно разделить на:

· безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

· неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;

· опасные вирусы, которые могут привести к серьезным сбоям в работе;

· очень опасные, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

Известны случаи, когда вирусы приводили к потере информации не только в масштабах одного или нескольких компьютеров, но и являлись причиной остановки работы крупных организаций.

По особенностям алгоритма можно выделить следующие группы вирусов:

· компаньон-вирусы (companion) - это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением .COM, например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет EXEфайл. При запуске такого файла DOS первым обнаружит и выполнит COM-файл, т.е. вирус, который затем запустит и EXE-файл.

· вирусы-“черви” (worm) - вирусы, которые распространяются в компьютерной сети и, так же как и компаньон-вирусы, не изменяют файлы или сектора на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии.

· “паразитические” - все вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу относятся все вирусы, которые не являются “червями” или “компаньон”.

· “студенческие” - крайне примитивные вирусы, часто нерезидентные и содержащие большое число ошибок;

· “стелс”-вирусы (вирусы-невидимки, stealth), представляющие собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и “подставляют” вместо себя незараженные участки информации.

Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие “обманывать” резидентные антивирусные мониторы.

· “полиморфик”-вирусы (самошифрующиеся или вирусы-призраки, polymorphic) - достаточно труднообнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

· “макро-вирусы” - вирусы этого семейства используют возможности макро-языков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). В настоящее время наиболее распространены макро-вирусы заражающие текстовые документы редактора Microsoft Word. Каким образом антивирусные программы защищают компьютер?

Антивирусные программы проверяют электронную почту и другие файлы компьютера на наличие вирусов, «червей» и «троянских коней». При обнаружении вируса, «червя» или «троянского коня» антивирусная программа либо отправляет вирус в карантин, либо полностью удаляет его до нанесения ущерба компьютеру и файлам. Некоторые компании, производящие антивирусные программы, предоставляют регулярное обновление антивирусных баз. Многие антивирусные программы имеют функцию автоматического обновления. При обновлении антивирусного про-

граммного обеспечения сведения о новых вирусах добавляются в список вирусов, на наличие которых выполняется проверка, обеспечивая защиту компьютера от новых атак.

При отсутствии автоматического антивирусного обновления рекомендуется производить эту процедуру регулярно, так как новые вирусы появляются ежедневно. Если используемая антивирусная программа требует подписки, настоятельно рекомендуется поддерживать подписку в активном состоянии для получения регулярных обновлений. Устаревший список вирусов подвергает компьютер новым угрозам безопасности.

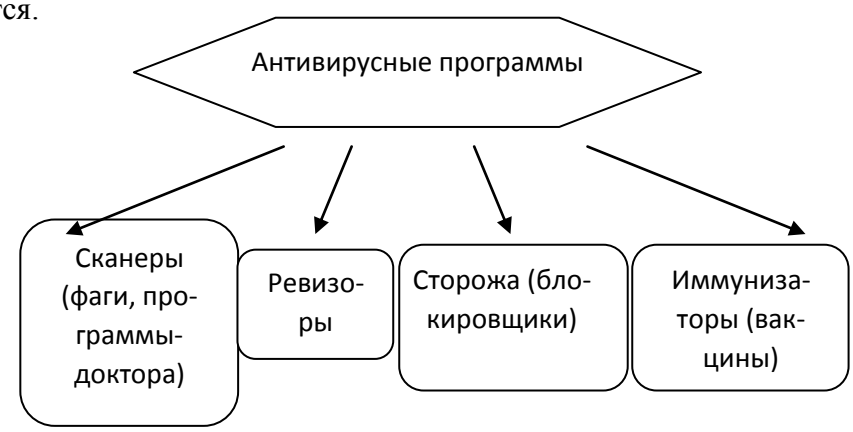
Различают следующие виды антивирусных программ:

Программы-мониторы. Резидентные программы, находящиеся постоянно в оперативной памяти компьютера и отслеживающие все файловые операции в системе. Позволяют обнаружить и удалить вирус до момента реального заражения системы в целом.

Программы-сканеры. Осуществляют поиск вируса по запросу пользователя на конкретно указанных дисках, папках или файлах.

Программы-доктора или фаги. Они не только находят заражённые файлы, но и удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. Среди фагов выделяют полифаги – программы, предназначенные для поиска и уничтожения большого количества вирусов, например Doctor Web или Norton AntiVirus.

Программы- вакцины или иммунизаторы. Это 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 заражёнными и поэтому не внедрится.



Почему необходимо бороться с компьютерными вирусами? Хотя вирусные атаки случаются не очень часто, общее число вирусов слишком велико, а ущерб от “хулиганских” действий вируса в системе может оказаться значительным. Существуют вирусы, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных 6 областях памяти, привести к серьезным сбоям в работе компьютера.

В результате этих действий Вы можете навсегда потерять данные, необходимые для работы и понести существенный моральный и материальный ущерб. “Эпидемия” компьютерного вируса в организации (неважно - большой или маленькой) может полностью дестабилизировать ее работу. При этом может произойти сбой в работе, как отдельных компьютеров, так и компьютерной сети в целом, что повлечет за собой потерю информации, необходимой для нормальной работы и потерю времени, которое будет затрачено на восстановление данных и приведением компьютеров и/или сети в рабочее состояние.

Возможные симптомы вирусного поражения:

Замедление работы некоторых программ.

Увеличение размеров файлов (особенно выполняемых).

Появление не существовавших ранее “странных” файлов.

Уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы).

Внезапно возникающие разнообразные видео и звуковые эффекты.

При всех перечисленных выше симптомах, а также при других “странных” проявлениях в работе системы (неустойчивая работа, частые “самостоятельные” перезагрузки и прочее) рекомендуется, немедленно произвести проверку Вашей системы на наличие вирусов. При этом лучше, если программа будет иметь самую последнюю версию и самые свежие обновления антивирусных баз.

Методы защиты от компьютерных вирусов:

Предотвращение поступления вирусов;

Предотвращение вирусной атаки, если вирус все-таки попал в компьютер;

Предотвращение разрушительных действий, если атака произошла.

Для реализации защиты существует три метода:

программные методы защиты;

аппаратные методы защиты;

организационные методы защиты.

Как предотвратить поступление компьютерных вирусов Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика.

Компьютерная профилактика состоит из небольшого количества правил, соблюдение которых значительно снижает вероятность заражения вирусом и утери каких-либо данных:

· Обязательно делайте регулярное резервное копирование.

· Покупайте дистрибутивные копии программного обеспечения у официальных продавцов.

· Периодически сохраняйте файлы, с которыми ведется работа, на внешний носитель.

· Проверяйте перед использованием флэшку. Не запускайте непроверенные файлы, в том числе полученные по компьютерным сетям.

· Ограничьте круг лиц, допущенных к работе на конкретном компьютере.

· Периодически проверяйте компьютер на наличие вирусов. При этом пользуйтесь свежими версиями антивирусных программ.

Если вирус попал в компьютер основное средство защиты информации – это резервное копирование наиболее важных данных. Резервные копии хранят на внешних носителях. Даже в случае полной потери данных на жёстком диске последствия не будут катастрофичными. Жёсткий диск придётся переформатировать, затем на него установить операционную систему с дистрибутивного компакт-диска, затем под её управлением установить необходимое программное обеспечение (тоже с дистрибутивных носителей). Завершается процесс восстановлением данных с резервных носителей.

Программные средства антивирусной защиты:

1. Создание образа жёсткого диска на внешних носителях. В случае выхода из строя данных в системных областях жёсткого диска сохранённый «образ диска» может позволить восстановить если не все данные, то большую их часть. Это же средство поможет от потери данных при аппаратных сбоях или при неаккуратном форматировании жёсткого диска.

2. Регулярное сканирование жёсткого диска в поисках компьютерных вирусов. Сканирование выполняется автоматически при каждом включении компьютера, но следует иметь в виду, что вирус отыскивают путём сравнения кода программ с кодами известных вирусов, хранящимися в базе данных.

3. Если база данных устарела, а вирус является новым, сканирующая программа его не обнаружит. Поэтому следует регулярно (раз в 2 недели) обновлять базу данных.

4. Контроль за изменением размеров и других атрибутов файлов. Поскольку некоторые вирусы, размножаясь, изменяют параметры заражённых файлов, контролирующая программа обнаружит их действия и предупредит пользователя.

5. Контроль за обращениями к жесткому диску. Поскольку наиболее опасные вирусы модифицируют данные, записанные на жёстком диске, антивирусные программы могут контролировать обращения к нему и предупредить пользователя о подозрительной активности.

Вспомогательными средствами защиты информации являются антивирусные программы и средства аппаратной защиты. При работе в Интернете следует иметь в виду, что насколько ресурсы Всемирной сети открыты каждому клиенту, настолько же и ресурсы его компьютерной системы могут быть при определенных условиях открыты всем, кто обладает необходимыми средствами. Для частного пользователя этот факт не играет особой роли, но знать о нем необходимо, чтобы не допускать действий, нарушающих законодательства тех стран, на территории которых расположены серверы Интернета.

К таким действиям относятся вольные или невольные попытки нарушить работоспособность компьютерных систем, попытки взлома защищенных систем, использование и распространение программ, нарушающих работоспособность компьютерных систем (в частности, компьютерных вирусов).

Работая во Всемирной сети, следует помнить о том, что абсолютно все действия фиксируются и протоколируются специальными программными средствами и информация как о законных, так и о незаконных действиях обязательно где-то накапливается. Таким образом, к обмену информацией в Интернете следует подходить как к обычной переписке с использованием почтовых открыток. Информация свободно циркулирует в обе стороны, но в общем случае она доступна всем участникам информационного процесса. Это касается всех служб Интернета, открытых для массового использования.

Полностью «отсечь» вирусы от вашего компьютера вряд ли удастся, разве что вы удалите из системы дисковод, перестанете работать в Интернет и будете пользоваться только легальным программным обеспечением.

Остается другой способ: снабдить вашу операционную систему надежными сторожами — антивирусными программами, которые смогут вовремя распознать и обезвредить вирус.

Практически все программы просты и удобны в пользовании, способны отлавливать практически все существующие сегодня группы вирусов. Большинство антивирусов способны не просто проверять по запросу пользователя диск на наличие вирусов, но и вести незаметную проверку всех запускаемых на компьютере файлов. Наконец, все современные антивирусы снабжены механизмом автоматического обновления антивирусных баз данных через Интернет.

Антивирусная база данных. Каждый файл имеет в коде особый участок - сигнатуру. У каждого файла он особый. Антивирусная лаборатория, "изловив" образец нового вредоносного кода, дизассемблирует его и выделяет сигнатуру. После этого сигнатура добавляется в специальную базу данных, где хранятся сигнатуры других вирусов. База находится на сервере лаборатории. При обновлении антивирус, установленный на компьютере пользователя (программаклиент) обновляет базу сигнатур на этом ПК. При сканировании диска движок антивируса сверяет сигнатуру проверяемого файла с базой сигнатур, которых порядка сотен тысяч. Бывает, что при выборе команды "Лечить" антивирус говорит, что лечение невозможно. Вирусы, поражая файл, часто переписывают его код и первичный код не сохраняют. Поэтому изменённый участок кода невозможно восстановить ("вылечить"). В таких случаях следует безжалостно удалять файл.

Троянские программы (Trojans) Программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к «зависанию», воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом «полезного» программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

В последнее время наиболее распространенными типами вредоносных программ, портящими компьютерные данные, стали черви. Далее по распространенности следуют вирусы и троянские

программы. Некоторые вредоносные программы совмещают в себе характеристики двух или даже трех из перечисленных выше классов.

Программы-рекламы (Adware) Программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе, изменяют различные параметры браузера (стартовые и поисковые страницы, уровни безопасности и т.д.), а также создают неконтролируемый пользователем трафик. Все это может привести как к нарушению политики безопасности, так и к прямым финансовым потерям.

Программы-шпионы (Spyware) Программное обеспечение, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О наличии программ-шпионов на своем компьютере вы можете и не догадываться. Как правило, целью программ-шпионов является: отслеживание действий пользователя на компьютере; сбор информации о содержании жесткого диска; в этом случает чаще всего речь идет о сканировании некоторых каталогов и системного реестра с целью составления списка программного обеспечения, установленного на компьютере; сбор информации о качестве связи, способе подключения, скорости модема и т.д.

Потенциально опасные приложения (Riskware) К потенциально опасным относятся приложения, которые не имеют вредоносных функций, но могут являться частью среды разработки вредоносного программного обеспечения или использоваться злоумышленниками в качестве вспомогательных компонентов вредоносных программ.

Программы-маскировщики (Rootkit) Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Программы-маскировщики модифицируют операционную систему на компьютере и заменяют основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Прочие опасные программы. Программы, созданные для организации DoS-атак на удаленные серверы, взлома других компьютеров, а также являющиеся частью среды разработки вредоносного программного обеспечения. К таким программам относятся хакерские утилиты (Hack Tools), конструкторы вирусов, сканеры уязвимостей, программы для взлома паролей, прочие виды программ для взлома сетевых ресурсов или проникновения в атакуемую систему.

Хакерские атаки. Хакерские атаки – это действия злоумышленников или вредоносных программ, направленные на захват информационных данных удаленного компьютера, выведение системы из строя или получение полного контроля над ресурсами компьютера.

Некоторые виды интернет-мошенничества Фишинг (Phishing) – вид интернет-мошенничества, заключающийся в рассылке электронных сообщений с целью кражи конфиденциальной информации, как правило, финансового характера.

Фишинг-сообщения составляются таким образом, чтобы максимально походить на информационные письма от банковских структур, компаний известных брендов. Письма содержат ссылку на заведомо ложный сайт, специально подготовленный злоумышленниками и являющийся копией сайта организации, якобы от имени которой пришло письмо. На данном сайте пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию. Дозвон на платные интернет-ресурсы – вид интернет-мошенничества, связанный с несанкционированным использованием платных интернет-ресурсов (чаще всего это вебсайты порнографического содержания). Установленные злоумышленниками программы (dialers) инициируют модемное соединение с вашего компьютера на платный ресурс, в результате пользователь вынужден оплачивать огромные счета.

Навязчивая реклама. Навязчивая реклама – это всплывающие окна и рекламные баннеры, открывающиеся при работе с веб-сайтами. Как правило, информация, содержащаяся в них, не бывает полезной. Демонстрация всплывающих окон и баннеров отвлекает пользователя от основных задач, увеличивает объем трафика.

Спам (Spam) Спам – это анонимная массовая рассылка нежелательных почтовых сообщений. Так, спамом являются рассылки рекламного, политического и агитационного характера, письма, призывающие помочь кому-нибудь. Отдельную категорию спама составляют письма с предложениями обналичить большую сумму денег или вовлекающие в финансовые пирамиды, а также письма, направленные на кражу паролей и номеров кредитных карт, письма с просьбой переслать знакомым (например, письма счастья) и т.п. Спам существенно увеличивает нагрузку на почтовые серверы и повышает риск потери информации, важной для пользователя. Обнаружение и блокирование данных видов угроз Антивирусом Касперского осуществляется с помощью двух методов: реактивный – метод, основанный на поиске вредоносных объектов с помощью постоянно обновляемой базы сигнатур угроз. Для реализации данного метода необходимо хотя бы одно заражение, чтобы добавить сигнатуру угрозы в базу и распространить обновление баз.

Проактивный – метод, в отличие от реактивной защиты, строящийся не на анализе кода объекта, а на анализе его поведения в системе. Этот метод нацелен на обнаружение новых угроз, информации о которых еще нет в базах. Применение обоих методов Антивирусом Касперского обеспечивает комплексную защиту вашего компьютера от известных, а также новых угроз. Проактивная защита вашего компьютера Антивирус Касперского защищает не только от известных угроз, но и от новых, информация о которых отсутствует в базах сигнатур угроз.

Законодательные и правовые основы защиты компьютерной информации

Законодательный уровень - защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов, регулирующих отношения субъектов по защите информации, применение этих документов, надзор и контроль за их исполнением. Законодательная база должна обеспечивать ***основные функции***:

разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации;

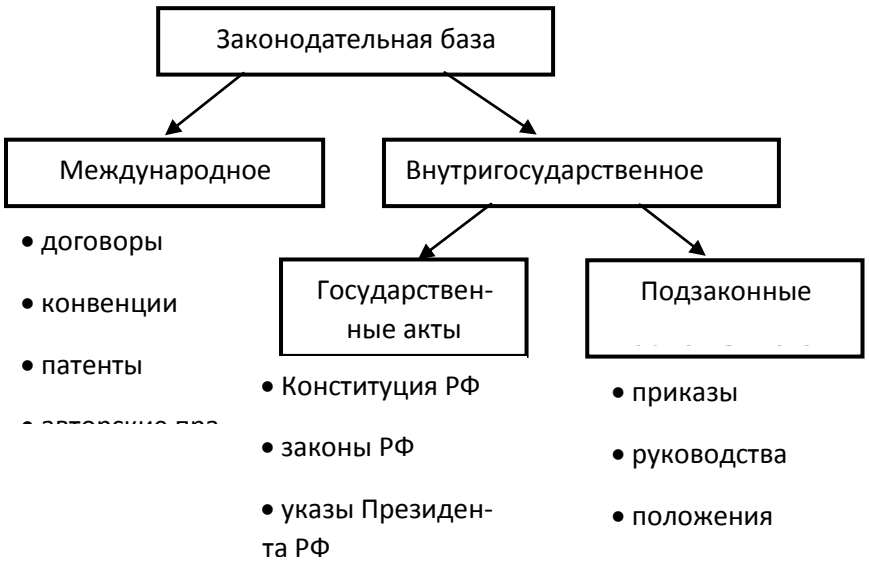
определение системы органов и должностных лиц, ответственных за обеспечение ИБ в стране и порядка регулирования деятельности предприятий и организаций в этой области4

создание полного комплекса нормативно-правовых руководящих и методических материалов регламентирующих вопросы обеспечения ИБ как в стране в целом, так и на конкретном объекте;

определение мер ответственности за нарушение правил защиты;

определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

В общем случае законодательная база гарантируется источниками международного и внутригосударственного права, содержание которых представлено на рисунке.



Основным законом РФ является Конституция принятая 12 декабря 1993 года.

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

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.

Статья 41 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.

Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам зашиты информации.

В настоящее время основополагающее значение в области ИБ имеют следующие ***законодательные акты***:

Гражданский кодекс Российской Федерации.

Уголовный кодекс Российской Федерации

Кодекс Российской Федерации об административных правонарушениях.

Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. № 646.

Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации»;

Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»

Федеральный закон № 63-ФЗ от 6 апреля 2011 г. «Об электронной подписи»;

Федеральный закон № 152-ФЗ от 27 июля 2006 г. «О персональных данных»;

Федеральный закон № 98-ФЗ от 29 июля 2004 г. «О коммерческой тайне»;

Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;

Закон РФ № 5485-1 от 21 июля 1993 г. «О государственной тайне».

Кодекс РФ об административных правонарушениях предусматривает ответственность за административные правонарушения в информационной сфере.

Уголовный Кодекс Российской Федерации предусматривает ответственность за информационные преступления.

Статья 137. Нарушение неприкосновенности частной жизни

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

Статья 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации

Статья 139. Нарушение неприкосновенности жилища

Статья 140. Отказ в предоставлении гражданину информации

Статья 155. Разглашение тайны усыновления (удочерении)

Статья 159.6. Мошенничество в сфере компьютерной информации

Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

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

Глава 28. Преступления в сфере компьютерной информации

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

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Статья 275. Государственная измена

Статья 276. Шпионаж

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Обладатель информации вправе: разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа; использовать информацию, в том числе распространять ее, по своему усмотрению; передавать информацию другим лицам по договору или на ином установленном законом основании; защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами; осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации обязан: соблюдать права и законные интересы иных лиц; принимать меры по защите информации; ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Ограничение доступа к информации устанавливается **федеральными законами** в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является **соблюдение конфиденциальности информации**, доступ к которой ограничен федеральными законами.

Информация **в зависимости от категории доступа** к ней подразделяется на: общедоступную информацию; информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация **в зависимости от порядка ее предоставления или распространения** подразделяется на: информацию, свободно распространяемую; информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях; информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению; информацию, распространение которой в РФ ограничивается или запрещается.

Все государственные информационные ресурсы РФ являются открытыми и общедоступными. В соответствии с законом РФ **«Об информации, информационных технологиях и защите информации»** определяются основные принципы доступности информации:

1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

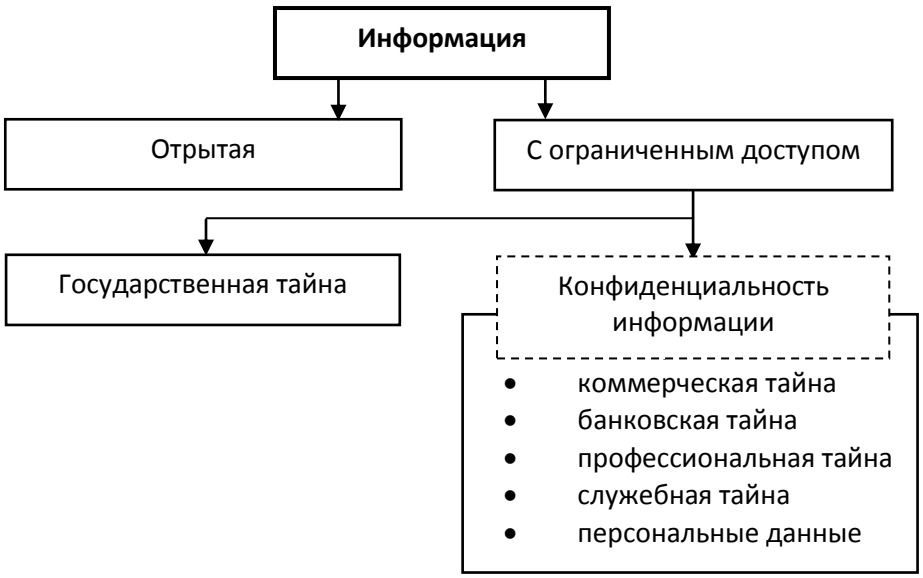
2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

3. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Исключение для доступности составляет документированная информация, отнесенная законом к **категории ограниченного доступа**.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. **Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными зако-**

нами. Классификация различных видов информации в зависимости от видов доступа представлена на рисунке.



Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.

Законодательство РФ о государственной тайне основывается на Конституции РФ, Законе РФ «О безопасности» и включает Закон «О государственной тайне», а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

Перечень сведений, составляющих государственную тайну, - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

о фактах нарушения прав и свобод человека и гражданина;

о размерах золотого запаса и государственных валютных резервах РФ;

о состоянии здоровья высших должностных лиц РФ;

о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

Коммерческая тайна - конфиденциальная информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну, - технологическая, производственная, научно-техническая, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений закона «О коммерческой тайне». Примерный состав информационных ресурсов, который целесообразно относить к сведениям, составляющим коммерческую тайну, представлен на рисунке.

Законом «О коммерческой тайне» определены сведения, которые **не могут составлять коммерческую тайну:**

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

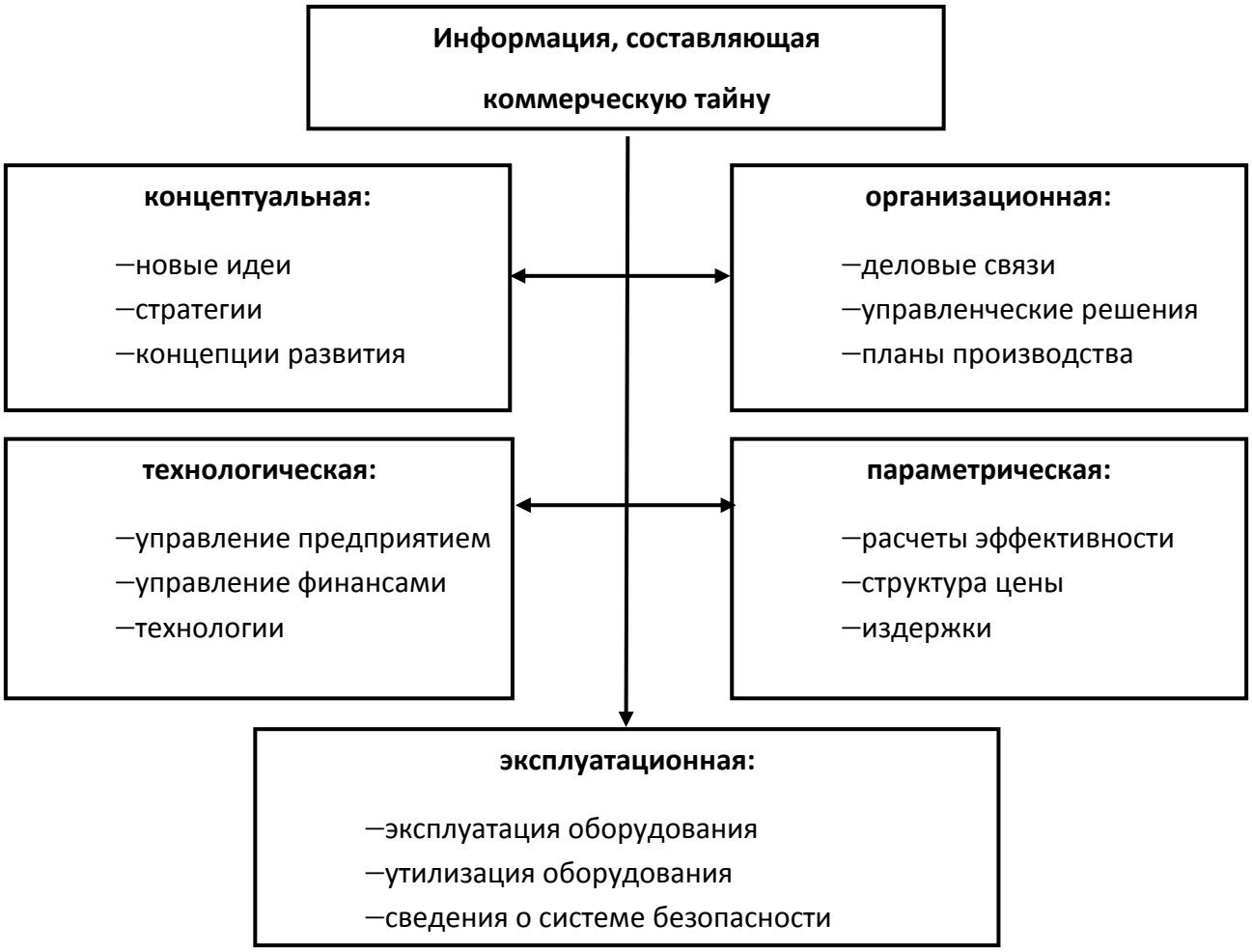
8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.



В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию обязаны предоставить эту информацию по запросу судов, органов прокуратуры, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

На документах, предоставляемых органам государственной власти и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф «Коммерческая тайна» с указанием ее обладателя (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Банковская тайна — защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

К основным объектам банковской тайны относятся следующие:

1. Тайна банковского счета — сведения о счетах клиентов и корреспондентов и действиях с ними в кредитной организации (о расчетном, текущем, бюджетном, депозитном, валютном, корре-

спондентском и тому подобных счетах, об открытии, закрытии, переводе, переоформлении счетов и т. д.).

2. Тайна операций по банковскому счету — сведения о принятии и зачислении поступающих на счет клиента денежных средств, о выполнении его распоряжений по перечислению и выдаче соответствующих сумм со счета, а также проведении других операций и сделок по банковскому счету, предусмотренных договором банковского счета или законом.

3. Тайна банковского вклада — сведения обо всех видах вкладов клиента в кредитной организации.

4. Тайна частной жизни клиента или корреспондента — сведения, составляющие личную, семейную тайну и охраняемые законом как персональные данные этого клиента или корреспондента.

Профессиональная тайна — защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Можно выделить следующие объекты профессиональной тайны:

1. ***Врачебная тайна*** — информация, содержащая:

–результаты обследования лица, вступающего в брак;

–сведения о факте обращения за медицинской помощью, о состоянии здоровья, диагнозе заболевания и иные сведения, полученные при обследовании и лечении гражданина;

–сведения о проведенных искусственном оплодотворении и имплантации эмбриона, а также о личности донора;

–сведения о доноре и реципиенте при трансплантации органов и (или) тканей человека;

–сведения о наличии психического расстройства, фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья гражданина;

–иные сведения в медицинских документах гражданина.

2. ***Тайна связи*** — тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

3. ***Нотариальная тайна*** — сведения, доверенные нотариусу в связи с совершением нотариальных действий.

4. ***Адвокатская тайна*** — сведения, сообщенные адвокату гражданином в связи с оказанием ему юридической помощи.

5. ***Тайна усыновления*** — сведения об усыновлении ребенка, доверенные на законном основании иным лицам, кроме судей, вынесших решение об усыновлении, и должностных лиц, осуществляющих государственную регистрацию этого усыновления.

6. ***Тайна страхования*** — сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц, полученные страховщиком в результате своей профессиональной деятельности.

7. ***Тайна исповеди*** — сведения, доверенные гражданином священнослужителю на исповеди.

Служебная тайна — защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Служебная тайна является видом конфиденциальной информации, и право на служебную тайну выступает самостоятельным объектом права. Для осуществления ее правовой охраны и защиты необходим специальный Федеральный закон «О служебной тайне».

Таким образом, к основным объектам служебной тайны можно отнести такие виды информации, как:

1. Служебная информация о деятельности федеральных государственных органов, доступ к которой ограничен федеральным законом в целях защиты государственных интересов: военная тайна;

2. Тайна следствия (данные предварительного расследования либо следствия); судебная тайна (тайна совещания судей, содержание дискуссий и результатов голосования закрытого совещания Конституционного суда Российской Федерации, материалы закрытого судебного заседания, тайна совещания присяжных заседателей или в силу служебной необходимости, порядок выработки и принятия решения, организация внутренней работы и т. д.);

3. Конфиденциальная информация, ставшая известной в силу исполнения служебных обязанностей должностным лицам государственных органов и органов местного самоуправления: коммерческая тайна, банковская тайна, профессиональная тайна, а также конфиденциальная информация о частной жизни лица.

В действующем законодательстве приводится перечень сведений, которые **не могут быть отнесены к служебной информации ограниченного распространения**:

– акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

– сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

– описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

– порядок рассмотрения и разрешения заявлений, в том числе юридических лиц, рассмотренных в установленном порядке;

– сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

– документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

Особенность правоотношений в этой области состоит в том, что если во втором случае государственные органы и их должностные лица обязаны обеспечить (гарантировать) сохранность «чужой» тайны, ставшей известной им по службе, в объеме сведений, переданных ее владельцем, то в первом случае они самостоятельно в соответствии с законом определяют объем своей служебной тайны и режим ее защиты.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Законодательство РФ в области персональных данных основывается на Конституции РФ и международных договорах РФ и состоит из Федерального закона «О персональных данных» и других определяющих случаи и особенности обработки персональных данных федеральных законов.

Обработка персональных данных должна осуществляться на основе принципов:

1) законности целей и способов обработки персональных данных и добросовестности;

2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

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.

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев:

1) обезличивания персональных данных;

2) в отношении общедоступных персональных данных.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных законодательством.

Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения.

Авторское право распространяется как на обнародованные произведения, так и на необнародованные произведения, существующие в какой-либо объективной форме:

письменной (рукопись, машинопись, нотная запись и так далее);

устной (публичное произнесение, публичное исполнение и так далее);

звуко- или видеозаписи (механической, магнитной, цифровой, оптической и так далее);

изображения (рисунок, картина, план, чертеж, кино-, теле-, видео- или фотокадр и т.д.);

объемно - пространственной (скульптура, модель, макет, сооружение и так далее);

в других формах.

Авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты. Авторское право на произведение не связано с правом собственности на материальный объект, в котором произведение выражено.

Объектами авторского права являются:

литературные произведения (включая программы для ЭВМ);

драматические и музыкально - драматические произведения, сценарные произведения;

хореографические произведения и пантомимы;

музыкальные произведения с текстом или без текста;

аудиовизуальные произведения (кино-, теле- и видеофильмы, слайдфильмы, диафильмы и другие кино- и телепроизведения);

произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства;

произведения декоративно - прикладного и сценографического искусства;

произведения архитектуры, градостроительства и садово - паркового искусства;

фотографические произведения и произведения, полученные способами, аналогичными фотографии;

географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и к другим наукам;

другие произведения.

Охрана программ для ЭВМ распространяется на все виды программ для ЭВМ (в том числе на операционные системы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код.

К объектам авторского права также относятся:

производные произведения (переводы, обработки, аннотации, рефераты, резюме, обзоры, инсценировки, аранжировки и другие переработки произведений науки, литературы и искусства);

сборники (энциклопедии, антологии, базы данных) и другие составные произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

Производные произведения и составные произведения охраняются авторским правом независимо от того, являются ли объектами авторского права произведения, на которых они основаны или которые они включают.

Не являются объектами авторского права:

официальные документы (законы, судебные решения, иные тексты законодательного, административного и судебного характера), а также их официальные переводы;

государственные символы и знаки (флаги, гербы, ордена, денежные знаки и иные государственные символы и знаки);

произведения народного творчества;

сообщения о событиях и фактах, имеющие информационный характер.

Авторское право на произведение науки, литературы и искусства возникает в силу факта его создания. Для возникновения и осуществления авторского права не требуется регистрации произведения, иного специального оформления произведения или соблюдения каких-либо формальностей.

Обладатель исключительных авторских прав для оповещения о своих правах вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состоит из трех элементов:

латинской буквы "С" в окружности: ©;

имени (наименования) обладателя исключительных авторских прав;

года первого опубликования произведения.

При отсутствии доказательств иного автором произведения считается лицо, указанное в качестве автора на оригинале или экземпляре произведения.

Стандарты информационной безопасности

Рассмотрим стандарты и спецификации двух разных видов:

оценочных стандартов, направленных на классификацию информационных систем и средств защиты по требованиям безопасности;

технических спецификаций, регламентирующих различные аспекты реализации средств защиты.

Важно отметить, что между эти видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем".

Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года. Уже одно его название требует комментария. Речь идет не о без-

опасных, а о доверенных системах, то есть системах, которым можно оказать определенную степень доверия.

"Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию".

Очевидно, однако, что абсолютно безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

В "Оранжевой книге" доверенная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Обратим внимание, что в рассматриваемых Критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической). Вопросы доступности "Оранжевая книга" не затрагивает.

Степень доверия оценивается по двум основным критериям.

1. Политика безопасности - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности - это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

2. Уровень гарантированности - мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

Важным средством обеспечения безопасности является механизм подотчетности (протоколирования). Доверенная система должна фиксировать все события, касающиеся безопасности.

Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации.Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности. Доверенная вычислительная база - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности.

Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор.

Вообще говоря, компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

Основное назначение доверенной вычислительной базы - выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

Изолированность. Необходимо предупредить возможность отслеживания работы монитора.

Полнота. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. Ядро безопасности - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют периметром безопасности. Компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, - нет.

Согласно "Оранжевой книге", политика безопасности должна обязательно включать в себя следующие элементы:

произвольное управление доступом;

безопасность повторного использования объектов;

метки безопасности;

принудительное управление доступом.

"Критерии ..." Министерства обороны США открыли путь к ранжированию информационных систем по степени доверия безопасности.

В "Оранжевой книге" определяется четыре уровня доверия - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Всего имеется шесть классов безопасности - C1, C2, B1, B2, B3, A1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, ее политика безопасности и уровень гарантированности должны удовлетворять заданным требованиям, из которых мы упомянем лишь важнейшие.

Рекомендации X.800 . Следуя скорее исторической, чем предметной логике, мы переходим к рассмотрению технической спецификации X.800, появившейся немногим позднее "Оранжевой книги", но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем.

Рекомендации X.800 - документ довольно обширный. Мы остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их реализации защитных механизмах.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

Управление доступом. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

Конфиденциальность данных. Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем конфиденциальность трафика (это защита информации, которую можно получить, анализируя сетевые потоки данных).

Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с

подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" Самый полный и современный среди оценочных стандартов - "Критериев оценки безопасности информационных технологий" (издан 1 декабря 1999 года). Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

По историческим причинам данный стандарт часто называют "Общими критериями" (или даже ОК).

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от "Оранжевой книги", ОК не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные "программы" - задания по безопасности, типовые профили защиты и т.п.

Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, "с нуля", программы не пишут уже очень давно; оценка безопасности тоже вышла на сопоставимый уровень сложности, и "Общие критерии" предоставили соответствующий инструментарий.

Важно отметить, что требования могут быть параметризованы, как и полагается библиотечным функциям. Как и "Оранжевая книга", ОК содержат два основных вида требований безопасности:

функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;

требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного объекта оценки - аппаратно-программного продукта или информационной системы.

Руководящие документы: Классификация автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД) и Классификация межсетевых экранов (МЭ).

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Переходя к рассмотрению второго РД Гостехкомиссии России - Классификации межсетевых экранов - укажем, что данный РД представляется нам принципиально важным, поскольку в

нем идет речь не о целостном продукте или системе, а об отдельном сервисе безопасности, обеспечивающем межсетевое разграничение доступа.

Данный РД важен не столько содержанием, сколько самим фактом своего существования. Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется фильтрация информации. Это понятно: чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Значительное внимание в РД уделено собственной безопасности служб обеспечения защиты и вопросам согласованного администрирования распределенных конфигураций.

Формальные модели безопасности

На рисунке 1 представлена схема классификации и взаимосвязи положений математических моделей безопасности компьютерных систем.

Рисунок 1 – Классификация и взаимосвязи положений математических моделей безопасности компьютерных систем

Основную роль в методе формальной разработки системы играет модель безопасности (модель управления доступом, модель политики безопасности). **Целью этой модели является вы-**

ражение сути требований по безопасности к данной системе. Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информации.

Модель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты. Так как она является формальной, возможно осуществить доказательство различных свойств безопасности системы.

Хорошая модель безопасности обладает свойствами абстрактности, простоты и адекватности моделируемой системе. Основные понятия, используемые в моделях разграничения доступа:

Доступ к информации — ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации

Объект доступа — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

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

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Модель дискреционного доступа (DAC)

В рамках дискреционной модели контролируется доступ субъектов (пользователей или приложений) к объектам (представляющим собой различные информационные ресурсы: файлы, приложения, устройства вывода и т.д.).

Для каждого объекта существует субъект-владелец, который сам определяет тех, кто имеет доступ к объекту, а также разрешенные операции доступа. Основными операциями доступа являются READ (чтение), WRITE (запись) и EXECUTE (выполнение, имеет смысл только для программ).

Таким образом, в модели дискреционного доступа для каждой пары субъект-объект устанавливается набор разрешенных операций доступа. При запросе доступа к объекту, система ищет субъекта в списке прав доступа объекта и разрешает доступ, если субъект присутствует в списке и разрешенный тип доступа включает требуемый тип. Иначе доступ не предоставляется.

Классическая система дискреционного контроля доступа является «закрытой» в том смысле, что изначально объект не доступен никому, и в списке прав доступа описывается набор разрешений. Также существуют «открытые» системы, в которых по умолчанию все имеют полный доступ к объектам, а в списке доступа описывается набор ограничений.

В частности, в Linux для каждого файла (все ресурсы в ОС Linux представимы в виде файлов, в том числе устройства ввода-вывода) устанавливаются разрешения доступа для трех категорий субъектов: владелец файла, члены той же группы, что и владелец, и все остальные пользователи. Для каждой из этих категорий устанавливаются права на чтение (r), запись (w) и выполнение (x). Набор прав доступа объекта может быть представлен в виде символьной строки. Например, запись «rwxr-xr--» означает, что владелец файла может делать с ним все, что угодно; члены его группы могут читать и исполнять файл, но не могут записывать, а прочим пользователям доступно только чтение.

Недостаток модели DAC заключается в том, что субъект, имеющий право на чтение информации может передать ее другим субъектам, которые этого права не имеют, без уведомления владельца объекта. Таким образом, нет гарантии, что информация не станет доступна субъектам, не имеющим к ней доступа. Кроме того, не во всех АИС каждому объекту можно назначить владельца (во многих случаях данные принадлежат не отдельным субъектам, а всей системе) .

Модель безопасности Белла-Ла Падулы

Одна из наиболее известных моделей безопасности — модель Белла-Ла Падулы (модель мандатного управления доступом). В ней определено множество понятий, связанных с контролем доступа; даются определения субъекта, объекта и операции доступа, а также математический аппарат для их описания. Эта модель в основном известна двумя основными правилами безопасности: одно относится к чтению, а другое – к записи данных.

Пусть в системе имеются данные (файлы) двух видов: секретные и несекретные, а пользователи этой системы также относятся к двум категориям: с уровнем допуска к несекретным данным (несекретные) и с уровнем допуска к секретным данным (секретные).

1. Свойство простой безопасности: несекретный пользователь (или процесс, запущенный от его имени) не может читать данные из секретного файла.

2. Свойство или свойство ограничения: пользователь с уровнем доступа к секретным данным не может записывать данные в несекретный файл. Это правило менее очевидно, но не менее важно.

Действительно, если пользователь с уровнем доступа к секретным данным скопирует эти данные в обычный файл (по ошибке или злому умыслу), они станут доступны любому «несекретному» пользователю. Кроме того, в системе могут быть установлены ограничения на операции с секретными файлами (например, запрет копировать эти файлы на другой компьютер, отправлять их по электронной почте и т.д.). Второе правило безопасности гарантирует, что эти файлы (или даже просто содержащиеся в них данные) никогда не станут несекретными и не «обойдут» эти ограничения. Таким образом, вирус, например, не сможет похитить конфиденциальные данные.

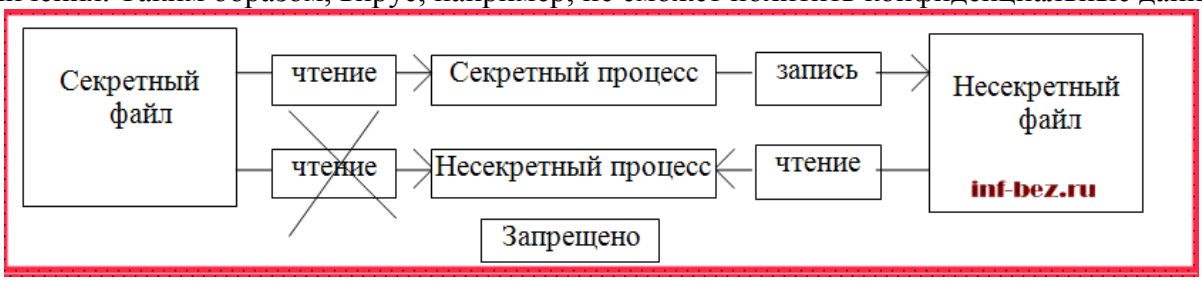


Рисунок 2 – Модель безопасности Белла-Ла Падулы

Рассмотренные правила легко распространить на случай, когда в системе необходимо иметь более двух уровней доступа — например, различаются несекретные, конфиденциальные, секретные и совершенно секретные данные. Тогда пользователь с уровнем допуска к секретным данным может читать несекретные, конфиденциальные и секретные документы, а создавать — только секретные и совершенно секретные.

Общее правило звучит так: пользователи могут читать только документы, уровень секретности которых не превышает их допуска, и не могут создавать документы ниже уровня своего допуска. То есть теоретически пользователи могут создавать документы, прочесть которые они не имеют права.

Модель Белла-Ла Падулы стала первой значительной моделью политики безопасности, применимой для компьютеров, и до сих пор в измененном виде применяется в военной отрасли. Модель полностью формализована математически. Основной упор в модели делается на конфиденциальность, но кроме неё фактически больше ничего не представлено. Кроме того, в модели игнорируется проблема изменения классификации: предполагается, что все сведения относятся к соответствующему уровню секретности, который остается неизменным. Наконец, бывают случаи, когда пользователи должны работать с данными, которые они не имеют права увидеть.

Ролевая модель контроля доступа (RBAC)

Ролевой метод управления доступом контролирует доступ пользователей к информации на основе типов их активностей в системе (ролей). Под ролью понимается совокупность действий и обязанностей, связанных с определенным видом деятельности. Примеры ролей: администратор базы данных, менеджер, начальник отдела.

В ролевой модели с каждым объектом сопоставлен набор разрешенных операций доступа для каждой роли (а не для каждого пользователя). В свою очередь, каждому пользователю сопоставлены роли, которые он может выполнять. В некоторых системах пользователю разрешается выполнять несколько ролей одновременно, в других есть ограничение на одну или несколько не противоречащих друг другу ролей в каждый момент времени.

Для формального определения модели RBAC используются следующие соглашения:

S = субъект — человек или автоматизированный агент.

R = роль — рабочая функция или название, определяется на уровне авторизации.

P = разрешения — утверждения режима доступа к ресурсу.

SE = сессия — Соответствие между S, R и/или P.

SA = назначение субъекта (Subject Assignment). $SA \subseteq S \times R$.

При этом субъекты назначаются связям ролей и субъектов в отношении «многие ко многим» (один субъект может иметь несколько ролей, а одну роля могут иметь несколько субъектов).

PA = назначение разрешения (Permission Assignment). $PA \subseteq P \times R$.

При этом разрешения назначаются связям ролей в отношении «многие ко многим».

RH = частично упорядоченная иерархия ролей (Role Hierarchy).

$PH \subseteq R \times R$.

На возможность наследования разрешений от противоположных ролей накладывается ограничительная норма, которая позволяет достичь надлежащего разделения режимов. Например, одному и тому же лицу может быть не позволено создать учетную запись для кого-то, а затем авторизоваться под этой учетной записью.

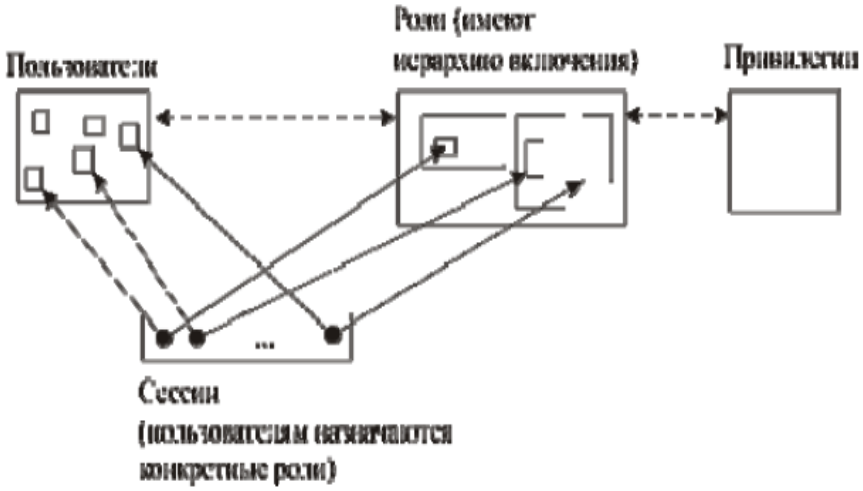


Рисунок 3 – Схема ролевой модели контроля доступа (RBAC)

При разработке модели для ПАО «Акцент-Банк» была взята именно ролевая модель контроля доступа, так как она обладает рядом достоинств по отношению к другим моделям. Среди них:

1. Простота администрирования. В отличие от модели DAC нет необходимости прописывать разрешения для каждой пары «объект-пользователь». Вместо этого прописываются разрешения для пар «объект-роль» и определяются роли каждого пользователя. При изменении области ответственности пользователя, у него просто изменяются роли.

2. Принцип наименьшей привилегии. Ролевая модель позволяет пользователю регистрироваться в системе ролью, минимально необходимой для выполнения требуемых задач. Запрещение полномочий, не требуемых для выполнения текущей задачи, не позволяет обойти политику безопасности системы.

3. Разделение обязанностей. RBAC широко используется для управления пользовательскими привилегиями в пределах единой системы или приложения. Список таких систем включает в себя Microsoft Active Directory, SELinux, FreeBSD, Solaris, СУБД Oracle, PostgreSQL 8.1, SAP R/3 и множество других, эффективно применяющих RBAC. С помощью RBAC могут быть смоделированы дискреционные и мандатные системы управления доступом .

Организационные методы защиты информации

Успешное решение комплекса задач по защите конфиденциальной информации не может быть достигнуто без создания единой основы, так называемого "активного кулака" предприятия, способного концентрировать все усилия, имеющиеся ресурсы для исключения утечки конфиденциальной информации и недопущения возможности нанесения ему ущерба.

Таким "кулаком" призвана стать система защиты информации на предприятии, создаваемая на нормативно-методической основе в данной области и отражающая все направления и специфику его деятельности.

Под системой защиты информации понимается совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях. Структура системы защиты информации приведена на рисунке 1.

Для решения организационных задач по созданию и функционирования системы защиты информации используются несколько основных подходов, которые вырабатываются на основе существующей нормативно-правовой базы и с учетом методических разработок по тем или иным направлениям защиты конфиденциальной информации.

Один из основных подходов к созданию системы защиты информации заключается во всестороннем анализе состояния защищенности информационных ресурсов предприятия с учетом устремленности конкурирующих организаций к овладению конфиденциальной информацией и, тем самым, нанесению ущерба предприятию. Важным элементом анализа является работа по определению перечня защищаемых информационных ресурсов с учетом особенностей их расположения (размещения) и доступа к ним различных категорий сотрудников (работников других предприятий).

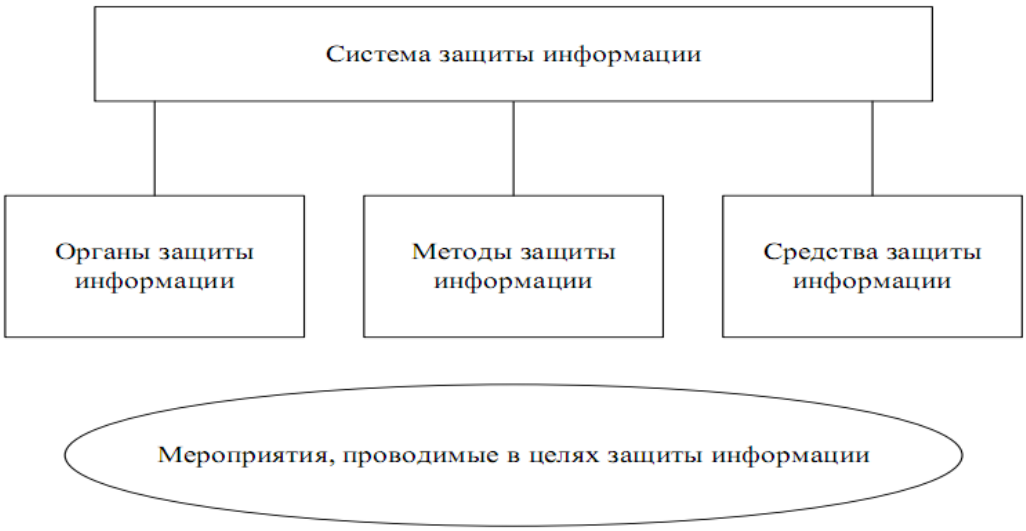


Рис. 1. Структура системы защиты информации

Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности. Изучение защищенности информационных ресурсов основывается на положительном и отрицательном опыте работы предприятия, накопленном в течение последних нескольких лет, а также наработанных деловых связях и контактах предприятия с организациями, осуществляющими аналогичные виды деятельности.

При создании системы защиты информации, в первую очередь, учитываются наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания. Предпочтение также отдается новым, перспективным направлениям деятельности предприятия, связанным с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность, а также развивающимся международным связям. На этой основе формируется

перечень возможных угроз информации, подлежащей защите, и определяются предполагаемые к использованию в этих целях конкретные силы, средства, способы и методы ее защиты.

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, стройность и эффективность.

Система защиты информации должна отвечать совокупности следующих основных требований, то есть быть:

централизованной - соответствующей эффективному процессу управления системой со стороны руководителя и ответственных должностных лиц по направлениям деятельности предприятия;

плановой - объединяющей усилия различных должностных лиц и структурных подразделений при их участии в организации и обеспечении выполнения задач, стоящих перед предприятием;

конкретной и целенаправленной - защите должны подлежать абсолютно конкретные информационные ресурсы, представляющие интерес для конкурирующих организаций;

активной - обеспечивать защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;

надежной и универсальной - охватывать весь комплекс деятельности предприятия, связанной с созданием и обменом информацией.

Одним из важнейших факторов, оказывающих существенное влияние на эффективность системы защиты конфиденциальной информации, является совокупность сил и средств предприятия, используемых для организации защиты информации и непосредственно участвующих в этом процессе.

Силы и средства различных предприятий отличаются по структуре, характеру и порядку использования. Предприятия, осуществляющие работу с конфиденциальной информацией и решающие задачи по ее защите на постоянной основе, то есть в каждодневной деятельности, вынуждены с этой целью создавать самостоятельные структурные подразделения и использовать высокоэффективные средства защиты информации.

Предприятиями, осуществляющими эпизодическую работу с конфиденциальной информацией, в силу ее небольших объемов, вместо создания вышеупомянутых подразделений в штаты своих предприятий могут включаться самостоятельные должности специалистов по защите информации.

Наряду с этим, данные предприятия на договорной основе могут использовать потенциал более крупных предприятий, имеющих необходимое количество квалифицированных сотрудников и высокоэффективные средства защиты информации. Эти вопросы регулируются нормативными актами, определяющими порядок оказания услуг в данной области.

Ведущую роль в организации защиты информации на предприятии играет руководитель предприятия, а также его заместитель, непосредственно возглавляющий эту работу.

Руководитель предприятия в соответствии с законодательством несет персональную ответственность за организацию и осуществление необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации.

Руководитель предприятия при организации работ по защите информации обязан:

- знать фактическое состояние дел по этим вопросам, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;
- определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;
- предъявлять высокую требовательность к сотрудникам предприятия в вопросах сохранности сведений конфиденциального характера;
- оценивать деятельность должностных лиц по защите информации и эффективность проводимых в целях защиты соответствующих сведений мероприятий.

Заместитель руководителя предприятия обязан постоянно изучать все стороны и направления деятельности предприятия с целью принятия своевременных мер по защите информации; руководить работой службы безопасности (структурных подразделений по защите государственной тайны), а также выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ.

В структуре предприятий с целью организации работ по защите информации могут создаваться следующие основные виды структурных подразделений:

- режимно-секретные;
- подразделения по противодействию иностранным техническим разведкам и технической защите информации;
- подразделения криптографической защиты информации;
- мобилизационные;
- подразделения охраны и пропускного режима.

Функции, возлагаемые на вышеперечисленные подразделения, определяются решением (приказом) руководителя предприятия и отражаются в соответствующих положениях.

По решению руководителя предприятия вышеупомянутые подразделения могут быть структурно объединены в службу режима предприятия, руководитель которой наделяется статусом заместителя руководителя предприятия, и полномочиями должностного лица, имеющего право осуществлять непосредственное руководство деятельностью всех подразделений предприятия, если их деятельность связана с использованием информации, отнесенной к конфиденциальной информации (государственной тайне) и подлежащей защите.

Кроме вышеперечисленных подразделений предприятия к работе по организации защиты информации могут привлекаться и иные структурные подразделения предприятия, основным направлением деятельности которых защита информации не является. Это - кадровые органы, органы юридической службы, органы психологической работы. Особо необходимо отметить участие в организации защиты информации производственных, так называемых "тематических" подразделений, непосредственно создающих продукцию, товары и услуги, и, в этой связи, непосредственно взаимодействующих с другими предприятиями и органами государственной власти.

При проведении работ по организации защиты информации используются и возможности различных нештатных подразделений предприятия, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области. Это - постоянно действующая техническая комиссия, экспертная комиссия, комиссия по рассекречиванию носителей конфиденциальной информации, комиссия по категорированию объектов автоматизации и другие.

Однако, для достижения наиболее эффективного результата при решении задач защиты конфиденциальной информации, наряду с использованием возможностей вышеупомянутых штатных и нештатных подразделений, необходимо комплексное применение имеющихся на предприятии средств защиты конфиденциальной информации.

Под средствами защиты информации понимаются технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, специальные средства, в которых они реализованы, а также средства, устройства и системы контроля эффективности защиты информации.

Общие методы защиты информации разделяются на правовые, организационно-технические и экономические.

Содержание правовых методов защиты информации направлено на решение следующих задач:

- разработку, совершенствование и обеспечение функционирования механизмов отнесения сведений к информации ограниченного доступа, засекречивания (рассекречивания) носителей информации, составляющей государственную тайну и иную охраняемую законом тайну, установления (снятия) ограничительных грифов для носителей конфиденциальной информации;
- определение перечней сведений, отнесенных к государственной (коммерческой) тайне;
- установление правового режима работы органов защиты информации;

- установление порядка доступа и допуска должностных лиц и граждан к государственной тайне и т.д.

Организационные методы защиты информации подразделяются по следующим классам:

- организация и соблюдение определенного порядка управленческой деятельности предприятия, направленная снижение риска утраты, утечки, модификации сведений конфиденциального характера;
- установление и соблюдение требований по организации и ведению конфиденциального делопроизводства, в том числе по размещению, оборудованию и охране;
- работа по ограничению (разграничению) круга должностных лиц предприятия по доступу к государственной тайне и конфиденциальной информации;
- осуществление принципа персональной ответственности должностных лиц за сохранность доверенной информации;
- организация подбора лиц, работающих с важной информацией их воспитание и обучение;
- систематический контроль за соблюдением режима защиты данных и оказание помощи подчиненным структурным подразделениям;
- мероприятия по сокращению оборота носителей секретной и конфиденциальной информации, систематический отбор и уничтожение ненужных носителей.

Таким образом, эффективное решение задач организации защиты информации невозможно без применения комплекса имеющихся в распоряжении руководителя предприятия методов защиты информации и соответствующих сил и средств.

Организация и функции службы безопасности предприятия. Внутриобъектовый и пропускной режимы устанавливаются на предприятиях, осуществляющих в предусмотренном законодательством РФ порядке работу со сведениями, составляющими государственную тайну.

Внутриобъектовый и пропускной режимы являются основными элементами системы защиты информации предприятия.

Их организация является обязательным условием соблюдения требований нормативно-методических документов по защите государственной (коммерческую) тайны, предоставляющим предприятию право на проведение в установленном порядке работ, связанных с использованием сведений, составляющих государственную (коммерческую) тайну.

Основными общими целями организации внутриобъектового и пропускного режимов на предприятии являются исключение (предотвращение):

- проникновения посторонних лиц на охраняемую (режимную) территорию и объекты предприятия, а также в служебные помещения, в которых проводятся работы с использованием сведений, составляющих государственную (коммерческую) тайну;
- посещения режимных помещений без служебной необходимости сотрудниками предприятия, не имеющими к ним прямого отношения, а также командированными лицами, не имеющими служебного задания на их посещение (работу в них);
- вноса (ввоза) на территорию предприятия личных технических средств: кино-, фото-, видео-, звукозаписывающей аппаратуры и других технических средств;
- несанкционированного выноса (вывоза) с территории предприятия носителей сведений, составляющих государственную (коммерческую) тайну;
- нарушений установленного регламента служебного времени, распорядка работы структурных подразделений по защите государственной (коммерческой) тайны, а также установленного порядка и режима работы сотрудников предприятия и командированных лиц с носителями сведений, составляющих государственную (коммерческую) тайну.

Организация и обеспечение внутриобъектового и пропускного режимов на предприятии в совокупности направлены на соблюдение всеми сотрудниками предприятия и командированными лицами надлежащего режима секретности.

Режим секретности - это установленный нормативными актами единый порядок обеспечения защиты сведений, составляющих государственную (коммерческую) тайну, включающий систему административно-правовых, организационных, инженерно-технических и других мер.

Таким образом, внутриобъектовый и пропускной режимы являются неотъемлемой частью системы установления и реализации комплекса мероприятий, направленных на защиту сведений, составляющих государственную (коммерческую) тайну, и сохранность их носителей.

Внутриобъектовый режим - совокупность комплекса мероприятий, направленных на обеспечение установленного режима секретности непосредственно в структурных подразделениях, на объектах и в служебных помещениях предприятия.

Основными целями внутриобъектового режима на предприятии являются:

- определение требований по общему режиму секретности на предприятии на основе положений нормативных правовых актов и указаний вышестоящих органов государственной власти (предприятий);
- ограничение круга лиц, допускаемых к сведениям, составляющим государственную (коммерческую) тайну, и их носителям;
- регламентация порядка и правил непосредственной работы сотрудников предприятия, а также командированных лиц, с носителями сведений, составляющих государственную (коммерческую) тайну;
- планирование комплекса мероприятий, направленных на исключение утечки сведений, составляющих государственную (коммерческую) тайну, и утрат носителей этих сведений;
- организация контроля со стороны должностных лиц предприятия и структурных подразделений по защите государственной (коммерческой) тайны за выполнением требований по режиму секретности на предприятии;
- организация работы с персоналом предприятия, допущенным к сведениям, составляющим государственную (коммерческую) тайну, а также с вновь принимаемыми на работу гражданами.

Задачи по организации внутриобъектового режима на предприятии возлагаются, как правило, на заместителя руководителя предприятия, отвечающего за вопросы защиты государственной (коммерческой) тайны. Заместитель руководителя предприятия работу по формированию внутриобъектового режима организует на основе всестороннего анализа возможных каналов утечки сведений, составляющих государственную (коммерческую) тайну, при проведении предприятием всех видов работ.

Важнейшую роль в организации внутриобъектового режима выполняют руководитель предприятия и его заместитель, в соответствии со своими должностными обязанностями непосредственно возглавляющий работу по защите государственной (коммерческой) тайны.

В соответствии с нормативными актами непосредственная ответственность за организацию и осуществление необходимых мероприятий по защите государственной (коммерческой) тайны возлагается на руководителя предприятия.

Основными структурными подразделениями предприятия, участвующими в организации внутриобъектового режима, являются: режимно-секретное подразделение, служба безопасности предприятия, подразделение противодействия техническим средствам разведки конкурента, подразделение охраны (в части вопросов контроля внутренних объектов и служебных помещений предприятия).

Обеспечение безопасности информации на наиболее уязвимых направлениях деятельности предприятия. В ходе повседневной деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну, и конфиденциальной информации, планируются и проводятся служебные совещания, в ходе которых рассматриваются или обсуждаются вопросы, содержащие конфиденциальную информацию.

Это могут быть вопросы, отнесенные к государственной тайне, касающиеся проводимых предприятием научно-исследовательских, опытно-конструкторских и иных видов работ, предусмотренных уставом предприятия, или вопросы, носящие конфиденциальный характер, отражающие коммерческую сторону деятельности предприятия.

Вышеперечисленные мероприятия могут быть внутренними (к участию в них привлекается только персонал данного предприятия) или внешними (с участием представителей сторонних организаций-партнеров).

Решение на проведение совещания во всех случаях принимается непосредственно руководителем предприятия или его заместителем по ходатайству руководителя подразделения, в чьих интересах оно будет проведено.

Принимаемые должностными лицами предприятия (структурным подразделением, его организующим) меры по защите конфиденциальной информации в ходе подготовки и проведения совещания должны носить как организационный, так и технический характер.

Мероприятия по защите информации проводятся при подготовке, в ходе проведения и по окончании совещания.

Одним из важных элементов в работе руководства и должностных лиц предприятия по защите информации при проведении совещания является этап планирования конкретных организационно-технических мер, направленных на исключение утечки конфиденциальной информации и на ее защиту.

Планирование мероприятий по защите информации включает выработку конкретных мер, определение ответственных за их реализацию должностных лиц (структурных подразделений) предприятия и сроков их выполнения (проведения).

Планирование мероприятий по защите информации, проводимых в ходе совещания с участием представителей сторонних организаций, осуществляется под руководством руководителя предприятия и при непосредственном участии его заместителя, возглавляющего на предприятии работу по защите информации. При отсутствии в структуре предприятия данного должностного лица, непосредственная ответственность за проведение планирования мероприятий по защите информации возлагается на руководителя режимно-секретного подразделения (службы безопасности).

Проведение совещания без приглашения представителей сторонних организаций может проводиться без участия режимно-секретного подразделения (службы безопасности). В этих случаях ответственность за планирование и проведение мероприятий по исключению утечки конфиденциальной информации и по ее защите возлагаются на руководителя структурного подразделения предприятия, организующего данное совещание.

При планировании совещания предусматривается такая очередность рассмотрения вопросов, при которой будет исключено участие в их обсуждении лиц, не имеющих к ним прямого отношения.

Непосредственная разработка плана подготовки и проведения совещания возлагается на структурное подразделение предприятия, организующее его проведение.

Подготовка плана осуществляется заблаговременно до начала совещания и включает мероприятия, проводимые перед проведением совещания, во время проведения совещания и по его завершении.

В плане указываются время и место проведения совещания, состав участников, перечень предприятий, участвующих в совещании.

План мероприятий по защите информации при подготовке и в ходе проведения совещания содержит следующие основные разделы:

1. Определение состава участников и их оповещение. В разделе отражаются: порядок формирования списка лиц, привлекаемых к участию в совещании, а также перечня предприятий, которым необходимо направить запросы с приглашениями; порядок подготовки и направления таких запросов; формирование содержания запросов.

2. Подготовка служебных помещений, в которых планируется проведение совещания. В разделе отражаются:

работа по выбору служебных помещений;

проверка соответствия помещений требованиям по защите информации;

необходимость и целесообразность принятия дополнительных организационно-технических мер, направленных на исключение утечки информации;

оборудование рабочих мест участников совещания, в том числе средствами автоматизации, на которых разрешена обработка конфиденциальной информации.

Определяется порядок использования средств звукоусиления, кино- и видеоаппаратуры (проекторов).

3. Определение объема обсуждаемой информации. В данном разделе отражаются: порядок определения перечня вопросов, выносимых на совещание, и очередности их рассмотрения; порядок оценки степени конфиденциальности вопросов; выделение вопросов, к которым допускается узкий круг лиц, участвующих в совещании.

4. Организация пропускного режима на территорию и в служебные помещения, в которых проводится совещание. В разделе отражаются вопросы организации и осуществления пропускного режима:

виды пропусков и проставляемых на них условных знаком (шифров) для прохода в конкретные служебные помещения; порядок учета, хранения, выдачи и выведения их из действия (сроки уничтожения);

режим прохода, посещения и пребывания в помещениях участников совещания.

Определяются количество и регламент работы основных и дополнительных контрольно-пропускных пунктов для прохода участников совещания на территорию и в служебные помещения.

5. Организация допуска участников совещания к рассматриваемым вопросам. Раздел содержит мероприятия, касающиеся непосредственного допуска участников к вопросам, выносимым на совещание, с учетом порядка их обсуждения и степени конфиденциальности информации, к которой допущен каждый участник совещания.

6. Осуществление записи (стенограммы), фото-, кино-, видеосъемки совещания. В разделе определяются порядок и возможные способы записи, съемки (стенографирования) хода совещания и обсуждаемых вопросов с учетом их конфиденциальности, а также должностные лица (подразделения), отвечающие за техническое обеспечение данного процесса.

7. Меры по защите информации непосредственно при проведении совещания. В разделе отражаются: порядок и способы охраны служебных помещений, меры по исключению прохода (проникновения) в них посторонних лиц, а также участников совещания, не участвующих в рассмотрении конкретных вопросов; мероприятия по предотвращению утечки информации по техническим каналам, силы и средства, задействованные при их проведении. Также определяются конкретные меры, исключающие визуальный просмотр и прослушивание ведущихся переговоров и обсуждения вопросов участниками совещания.

8. Организация учета, хранения, выдачи и рассылки материалов совещания. В разделе отражаются порядок учета, хранения, размножения (печатания, ксерокопирования), выдачи, рассылки и уничтожения материалов совещания, а также рабочих тетрадей (блокнотов), предназначенных для записи обсуждаемых вопросов участниками совещания. Определяется порядок обращения с данными носителями информации непосредственно в ходе совещания и после его окончания. Особое внимание уделяется порядку учета, хранения, размножения и использования материалов совещания, зафиксированных на магнитных носителях (исполненных в электронном виде).

9. Оформление документов лиц, принимавших участие в совещании. В данном разделе отражается порядок и сроки оформления документов, подтверждающих право доступа участников совещания к конфиденциальной информации, предписаний (доверенностей) на участие в совещании, командировочных удостоверений;

10. Проверка и обследование места проведения совещания после его окончания. Раздел содержит мероприятия по организации и проведению визуальной проверки, а также проверки с использованием специальных технических средств (аппаратуры) помещений, в которых проводилось совещание с целью выявления оставленных (забытых) технических устройств, носителей конфиденциальной информации и личных вещей участников совещания.

11. Организация контроля выполнения требований по защите информации. В разделе отражается порядок, способы и методы контроля полноты и качества проводимых мероприятий, направленных на предотвращение утечки сведений конфиденциального характера, разглашения

информации, содержащей такие сведения, и утрат (хищений) носителей информации. Указываются структурные подразделения (должностные лица), на которые возлагаются вопросы контроля.

Определяется система и порядок представления ответственными должностными лицами докладов о наличии носителей конфиденциальной информации и выявленных нарушениях в работе по защите конфиденциальной информации.

Для каждого включаемого в план мероприятия определяются: срок (время) его проведения и ответственное за выполнение мероприятия должностное лицо (подразделение).

При использовании в ходе совещания сведений конфиденциального характера или обсуждении вопросов, содержащих такие сведения, руководство предприятия-организатора, осуществляет комплекс мероприятий, направленных на исключение ознакомления с ней посторонних лиц и сотрудников фирм-конкурентов.

На совещание приглашаются работники, имеющие непосредственное отношением к рассматриваемым (обсуждаемым) вопросам.

При обсуждении в ходе совещания вопросов, содержащих сведения, составляющие государственную тайну, его участники должны иметь допуск к этим сведениям по соответствующей форме, а при рассмотрении вопросов, отнесенных к иным видам конфиденциальной информации, в установленном порядке оформленное решение руководителя предприятия на допуск к данной категории (виду) информации.

При последовательном рассмотрении вопросов, имеющих различную степень конфиденциальности, к участию в совещании по каждому из рассматриваемых вопросов допускаются лица, имеющие к ним непосредственное отношение.

Непосредственно перед началом совещания руководитель предприятия или должностное лицо, ответственное за его проведение, обязан проинформировать участников совещания о степени конфиденциальности обсуждаемых вопросов.

В ходе совещания, в том числе и во время перерывов, работник, ответственный за его проведение, совместно со службой безопасности (режимно-секретным подразделением) осуществляет необходимые организационно-технические мероприятия, направленные на исключение утечки сведений конфиденциального характера.

Во время перерывов в совещании, а также после завершения обсуждения одного вопроса и перехода к обсуждению следующего, сотрудники службы безопасности (службы охраны) организуют контроль прохода (нахождения) в служебные помещения, в которых проводится совещание, лиц в соответствии с утвержденным списком участников.

На все время проведения совещания запрещается пронос в служебные помещения, в которых оно проводится, индивидуальных видео- и звукозаписывающих устройств, а также средств связи (в том числе мобильных телефонов и приемников персонального вызова). В целях обеспечения их сохранности организуется камера хранения личных вещей участников совещания.

Звуко- и видеозапись, а также кино- и видеосъемка хода совещания и обсуждения вопросов совещания проводится с разрешения руководителя предприятия-организатора совещания только на учтенных в режимно-секретном подразделении (службе безопасности) носителях. При этом использование в этих целях соответствующей аппаратуры и технических устройств осуществляется при соблюдении требований по защите информации.

Носители конфиденциальной информации, а также сведений, составляющих государственную тайну, выдаются режимно-секретным подразделением (службой безопасности) участникам совещания под роспись, а после окончания совещания возвращаются. Контроль за своевременным возвратом этих носителей осуществляется сотрудниками вышеуказанных подразделений.

Для осуществления записей хода совещания и обсуждаемых вопросов участникам совещания установленным порядком выдаются рабочие тетради или рабочие блокноты, учтенные в службе безопасности (режимно-секретном подразделении) и имеющие соответствующий гриф секретности (степень конфиденциальности). Эти рабочие тетради (блокноты) по окончании совещания воз-

вращаются в службу безопасности (режимно-секретное подразделение). При необходимости они могут быть секретной (конфиденциальной) почтой направлены для дальнейшего хранения и использования на предприятия, представители которых производили в них записи на совещании.

Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия

В настоящее время невозможно представить деятельность современного предприятия без его участия в издательской деятельности и рекламных акциях различного характера. Вместе с тем, для предприятий, осуществляющих работу с конфиденциальной информацией, такие его виды деятельности могут привести к распространению охраняемой информации о направлениях его деятельности и проводимых работах.

В связи с этим, в повседневной деятельности предприятия мероприятия по защите информации в процессе подготовки и реализации рекламных и издательских проектов занимают важное место.

Основными направлениями защиты конфиденциальной информации в ходе осуществления предприятием рекламной деятельности являются:

- подготовка и экспертиза предполагаемых к распространению рекламных материалов на предмет отсутствия в них информации с ограниченным доступом;
- анализ материалов, подготавливаемых рекламопроизводителем и рекламораспространителем к размещению в средствах рекламы;
- постоянный контроль порядка выхода и содержания рекламных материалов независимо от способа, формы и периодичности их распространения.

При принятии руководителем предприятия решения на рекламирование деятельности предприятия, а также производимых им товарах или услугах должностное лицо, назначенное ответственным за подготовку рекламных материалов и их передачу рекламопроизводителю и (или) рекламораспространителю организует работу, направленную на предотвращение распространения в рекламе конфиденциальной информации. Комплекс мероприятий по защите информации включает проведение экспертизы предполагаемых к распространению материалов комиссией предприятия, анализ возможных форм, способов распространения рекламных материалов и непосредственное взаимодействие по вопросам организации и распространения материалов с рекламопроизводителем и рекламораспространителем.

Одним из важных элементов в этой работе является оценка комиссией предприятия, состоящей из компетентных специалистов, содержания материалов на предмет возможности их распространения, в том числе и объема этих материалов. После получения положительного заключения экспертной комиссии предприятия осуществляется подготовка договорных материалов на передачу рекламных материалов рекламопроизводителю и (или) рекламораспространителю а также непосредственная передача материалов, предполагаемых к рекламному распространению.

В дальнейшем предприятие осуществляет постоянный контроль содержания рекламы при ее выходе в свет.

Организация подготовки материалов к открытому опубликованию

С целью исключения распространения в средствах массовой информации сведений конфиденциального характера на предприятии планируется и проводится работа по анализу содержания материалов, предполагаемых к открытому распространению в средствах массовой информации.

Цель данной работы - недопущение утечки информации о деятельности предприятия, содержащей сведения с конфиденциального характера, а также сведений, составляющих государственную тайну, или служебную информацию ограниченного распространения (служебную тайну). Для достижения этой цели проводится комплекс организационных мероприятий. Планирование и осуществление данных мероприятий проводят: служба безопасности, структурное подразделение по защите государственной тайны или специально создаваемое в структуре предприятия подразделение (должностное лицо), на которое возлагаются вышеуказанные задачи.

Сотрудники предприятия, принимающие непосредственное участие в подготовке материалов к открытому опубликованию, должны знать и руководствоваться положениями статьи 5 Закона

РФ "О государственной тайне", "Перечнем сведений, отнесенных к государственной тайне", другими нормативными актами, а также перечнем информации, составляющей коммерческую тайну предприятия.

Подготовка материалов к открытому опубликованию включает в себя их разработку авторами, предварительную проверку их содержания руководителями структурных подразделений предприятия, согласование возможности опубликования материалов со службой безопасности (подразделением по защите государственной тайны) предприятия.

Подготовленные к открытому опубликованию материалы не должны содержать сведений, составляющих государственную, коммерческую тайну, служебной информации ограниченного распространения (сведений, содержащих служебную тайну) и иной информации с ограниченным доступом, определенной нормативными правовыми актами.

Организация работы с персоналом предприятия. В соответствии со статьей 6 Федерального закона РФ "Об информации, информационных технологиях и защите информации" вопросы ограничения доступа к информации, определения порядка и условий такого доступа отнесены к компетенции обладателя информации. Обладатель информации при осуществлении своих прав обязан ограничивать доступ к информации и принимать меры по ее защите, если такая обязанность установлена федеральными законами.

В настоящее время в нашем государстве законодательно урегулированы (определены) и подробно раскрыты вопросы допуска и доступа должностных лиц и граждан к сведениям, составляющим государственную или коммерческую тайну. Порядок допуска лиц к иным видам информации с ограниченным доступом с учетом положений Федерального закона РФ "Об информации, информационных технологиях и защите информации" находится в компетенции соответствующих должностных лиц (обладателей такой информации).

Доступ граждан к сведениям (информации), в установленном порядке отнесенным к коммерческой тайне, осуществляется в соответствии со статьями 7 и 10 Федерального закона РФ "О коммерческой тайне".

С момента установления в отношении информации, составляющей коммерческую тайну, режима коммерческой тайны, полномочия по принятию решения о доступе к ней, переходят к обладателю информации.

Необходимо отметить, что определение порядка доступа лиц к коммерческой тайне и учет лиц, получивших такой допуск, являются одними из мер по охране конфиденциальности такой информации, принятие которых для обладателя информации в соответствии с Федеральным законом РФ "О коммерческой тайне" является обязательным.

Меры по охране конфиденциальности информации признаются разумно достаточными, если исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя.

Иные, не противоречащие законодательству России меры по ограничению порядка доступа к коммерческой тайне, могут быть дополнительно приняты ее обладателем.

Одним из вопросов государственного регулирования в сфере защиты государственной тайны является порядок допуска и доступа должностных лиц и граждан к сведениям, составляющим государственную тайну. Эта область является наиболее значимой для решения задач по защите государственной тайны и, в связи с этим, будет в данном учебном пособии раскрыта подробнее.

Допуск и непосредственный доступ должностных лиц и граждан к сведениям, составляющим государственную тайну, и их носителям, осуществляется в соответствии с положениями Закона РФ "О государственной тайне" на основании "Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

Допуск граждан к государственной тайне осуществляется соответствующими руководителями органов государственной власти, предприятий и организаций.

Допуск граждан к государственной тайне осуществляется в добровольном порядке и предусматривает:

- принятие на себя допущенными к государственной тайне лицами обязательств перед госу-

дарством по нераспространению доверенных им сведений, составляющих государственную тайну;

- согласие на частичные временные ограничения их прав в соответствии с Законом РФ "О государственной тайне";

- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

- определение видов, размеров и порядка предоставления льгот, предусмотренных законодательством Российской Федерации;

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

- принятие соответствующего решения руководителем предприятия о допуске оформляемого лица к государственной тайне.

Должностное лицо или гражданин, допущенные (ранее допускавшиеся) к государственной тайне, могут быть временно ограничены в следующих своих правах:

- в праве на выезд за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;

- в праве на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;

- в праве на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

Ограничение гражданина в праве на выезд из Российской Федерации осуществляется в соответствии с Федеральным законом РФ "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию".

В целях частичной компенсации ограничений в правах для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:

- процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;

- преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями и организациями организационных и (или) штатных мероприятий.

Для сотрудников подразделений по защите государственной тайны дополнительно к вышеперечисленным льготам устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурных подразделениях.

Граждане, которым по характеру занимаемой ими должности необходим доступ к государственной тайне, могут быть назначены на эти должности (приняты на работу) только после оформления в установленном порядке допуска по соответствующей форме.

Перечень должностей, при назначении на которые граждане обязаны оформлять допуск к сведениям, составляющим государственную тайну, в связи с возложением на них соответствующих должностных (функциональных) обязанностей, определяется номенклатурой должностей. Номенклатура должностей разрабатывается предприятием, согласовывается с соответствующим органом Федеральной службы безопасности РФ, и после этого согласования утверждается руководителем предприятия (его заместителем, возглавляющим работу по защите государственной тайны).

Изменения и дополнения в номенклатуру должностей вносятся в установленном порядке по мере необходимости. Полная переработка номенклатуры должностей осуществляется не реже одного раза в 5 лет.

Порядок разработки, согласования, утверждения номенклатуры, а также внесения в нее изменений и дополнений определяются "Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

С целью подтверждения фактической работы (ознакомления) сотрудников предприятия со сведениями, составляющими государственную тайну, подразделение по защите государственной тайны ведет учет их осведомленности в этих сведениях.

Допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну.

В соответствии со степенями секретности сведений, составляющих государственную тайну, и грифами секретности их носителей, установлены следующие формы допуска:

первая форма - для граждан, допускаемых к сведениям особой важности;

вторая форма - для граждан, допускаемых к совершенно секретным сведениям;

третья форма - для граждан, допускаемых к секретным сведениям.

Проверочные мероприятия, связанные с допуском граждан к государственной тайне, осуществляются соответствующими органами безопасности во взаимодействии с органами, осуществляющими в соответствии с законодательством оперативно-розыскную деятельность.

Уровень необходимого допуска личного состава определяется степенью секретности сведений (грифом секретности их носителей), с которыми они знакомятся (работают) в рамках исполнения должностных обязанностей. Уровень допуска для каждого должностного лица, работающего на предприятии, отражается в Номенклатуре должностей.

Доступ к сведениям, составляющим государственную тайну - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, возлагается на руководителя соответствующего органа государственной власти, предприятия или организации, а также на их структурные подразделения по защите государственной тайны.

Руководитель предприятия обязан осуществлять постоянный контроль за соответствием формы допуска граждан степени секретности сведений, к которым они фактически имеют доступ.

Он несет персональную ответственность за создание таких условий, при которых должностное лицо или гражданин знакомятся только с теми сведениями, составляющими государственную тайну, и в таких объемах, которые необходимы ему для выполнения его должностных (функциональных) обязанностей.

Основанием для непосредственного доступа лица к сведениям, составляющим государственную тайну, и их носителям, является решение руководителя предприятия, оформляемое в карточке о допуске.

Персонал предприятия, допущенный в силу должностных (функциональных) обязанностей к сведениям конфиденциального характера, - основной субъект правоотношений в сфере защиты конфиденциальной информации. Одновременно он является и единственным ее "нематериальным носителем".

В решении проблемы комплексной защиты информации на предприятии все более значительное место занимает выбор эффективных способов и методов работы с персоналом предприятия. Персонал предприятия, являясь генератором новых идей, открытий и изобретений, ускоряющих научно-технический прогресс, направляет максимальные усилия на повышение благосостояния предприятия в целом и каждого его сотрудника в частности.

Вопросы охраны конфиденциальности информации, к которой допускается работник предприятия, закреплены в разделе III Трудового кодекса РФ.

В соответствии с его положениями в заключаемом работодателем с работником трудовом договоре могут предусматриваться условия о неразглашении работником охраняемой законом тайны (государственной, служебной, коммерческой и иной).

В работе с персоналом предприятия, допущенным к конфиденциальной информации, используются следующие методы:

- обучения;
- инструктажей;
- индивидуальной и воспитательной работы;
- проверки уровня знаний;
- контроля.

Программно-технические меры обеспечения защиты информации

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей — оборудования, программ и/или данных, образует последний и самый важный рубеж ИБ. Компьютеры помогли автоматизировать многие области человеческой деятельности. Даже физическую защиту все чаще поручают не охранникам, а интегрированным компьютерным системам, что позволяет одновременно отслеживать перемещения сотрудников и по организации, и по информационному пространству.

Следует, учитывать, что быстрое развитие информационных технологий не только предоставляет обороняющимся новые возможности, но и объективно затрудняет обеспечение надежной защиты, если опираться исключительно на меры программно-технического уровня. Причин тому несколько:

- повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет методом грубой силы преодолевать барьеры (прежде всего криптографические), ранее казавшиеся неприступными;
- развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют круг злоумышленников, имеющих техническую возможность организовывать атаки;
- появление новых информационных сервисов ведет и к образованию новых уязвимых мест как "внутри" сервисов, так и на их стыках;
- конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки, что приводит к снижению качества тестирования и выпуску продуктов с дефектами защиты;
- навязываемая потребителям парадигма постоянного наращивания мощности аппаратного и программного обеспечения не позволяет долго оставаться в рамках надежных, апробированных конфигураций и, кроме того, вступает в конфликт с бюджетными ограничениями, из-за чего снижается доля ассигнований на безопасность.

Центральным для программно-технического уровня является понятие сервиса безопасности:

1. идентификация и аутентификация;
2. управление доступом;
3. протоколирование и аудит;
4. шифрование;
5. контроль целостности;
6. экранирование;
7. анализ защищенности;
8. обеспечение отказоустойчивости;
9. обеспечение безопасного восстановления;
10. туннелирование;
11. управление.

Для проведения классификации сервисов безопасности и определения их места в общей архитектуре меры безопасности можно разделить на следующие виды:

- превентивные, препятствующие нарушениям ИБ;
- меры обнаружения нарушений;
- локализующие, сужающие зону воздействия нарушений;
- меры по выявлению нарушителя;
- меры восстановления режима безопасности.

С точки зрения безопасности наиболее существенными представляются следующие аспекты современных ИС:

- корпоративная сеть имеет несколько территориально разнесенных частей (поскольку организация располагается на нескольких производственных площадках), связи между которыми находятся в ведении внешнего поставщика сетевых услуг, выходя за пределы зоны, контролируемой организацией;

- корпоративная сеть имеет одно или несколько подключений к Internet;
- на каждой из производственных площадок могут находиться критически важные серверы, в доступе к которым нуждаются сотрудники, работающие на других площадках, мобильные пользователи и, возможно, сотрудники других организаций;
- для доступа пользователей могут применяться не только компьютеры, но и потребительские устройства, использующие, в частности, беспроводную связь;
- в течение одного сеанса работы пользователю приходится обращаться к нескольким информационным сервисам, опирающимся на разные аппаратно-программные платформы;
- к доступности информационных сервисов предъявляются жесткие требования, которые обычно выражаются в необходимости круглосуточного функционирования с максимальным временем простоя порядка нескольких минут;
- информационная система представляет собой сеть с активными агентами, то есть в процессе работы программные компоненты, такие как апплеты или сервлеты, передаются с одной машины на другую, и выполняются в целевой среде, поддерживая связь с удаленными компонентами;
- не все пользовательские системы контролируются сетевыми и/или системными администраторами организации; программное обеспечение, особенно полученное по сети, не может считаться надежным, в нем могут быть ошибки, создающие проблемы в защите;
- конфигурация информационной системы постоянно изменяется на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привилегии и версии программ, появляются новые сервисы, новая аппаратура и т.п.).

Архитектурная безопасность. Сервисы безопасности, какими бы мощными они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. Только проверенная архитектура способна сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

С практической точки зрения наиболее важными являются следующие принципы архитектурной безопасности:

непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;

следование признанным стандартам, использование апробированных решений;

иерархическая организация ИС с небольшим числом сущностей на каждом уровне;

усиление самого слабого звена;

невозможность перехода в небезопасное состояние;

минимизация привилегий;

разделение обязанностей;

эшелонированность обороны;

разнообразие защитных средств;

простота и управляемость информационной системы.

Для обеспечения высокой доступности (непрерывности функционирования) необходимо соблюдать следующие принципы архитектурной безопасности:

внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.);

наличие средств обнаружения нештатных ситуаций;

наличие средств реконфигурирования для восстановления, изоляции и/или замены компонентов, отказавших или подвергшихся атаке на доступность;

выделение подсетей и изоляция групп пользователей друг от друга. Данная мера, являющаяся обобщением разделения процессов на уровне операционной системы, ограничивает зону поражения при возможных нарушениях ИБ.

Идентификация и аутентификация. Идентификация и аутентификация – это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

В сетевой среде, когда стороны идентификации/аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

- что служит аутентификатором (то есть используется для подтверждения подлинности субъекта);
- как организован обмен данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

- нечто, что он знает (пароль, личный идентификационный номер и т.п.);
- нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев и т.п.).

В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения и/или воспроизведения данных.

Сервис идентификации/аутентификации может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

Главное достоинство парольной аутентификации — простота и привычность. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя.

Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

Пароль можно угадать "методом грубой силы", используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен).

Рассмотренные пароли можно назвать многоразовыми; их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются одноразовые пароли.

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться, программы или специальные интеллектуальные карты. Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронными.

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу

физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

Аутентификация по отпечаткам пальцев. В настоящее время существуют два возможных способа использования этого приема для аутентификации пользователя автоматизированной системы:

- непосредственное сравнение изображений отпечатков пальцев, полученных с помощью оптических устройств, с отпечатками из архива;
- сравнение характерных деталей отпечатка в цифровом виде, которые получают в процессе сканирования изображений отпечатка.

При непосредственном сравнении изображений отпечатков устройство аутентификации определяет оптическое соотношение двух изображений и вырабатывает сигнал, определяющий степень совпадения отпечатков. Сравнение отпечатков обычно выполняется непосредственно на месте установки устройства. Передача изображений отпечатка по каналам связи не применяется из-за ее сложности, высокой стоимости и необходимости дополнительной защиты этих каналов.

Большое распространение получил способ, построенный на сравнении деталей отпечатков (метод соотнесения бороздок на отпечатках). При этом пользователь вводит с клавиатуры идентифицирующую информацию, по которой устройство аутентификации проводит поиск необходимого списка деталей отпечатка в архиве. После этого он помещает палец на оптическое устройства, и начинается процесс сканирования, в результате которого вычисляются координаты 12 точек, определяющих относительное расположение бороздок отпечатка. Сравнение проводится в ЭВМ по специальным алгоритмам.

Аутентификация по форме кисти руки. Принцип действия таких устройств аутентификации основан на уникальности таких характеристик руки человека, как длина пальцев, закругленность их кончиков, прозрачность кожи и т.д. Информация об этих параметрах может получаться различными способами, например при освещении руки, помещенной на панель из фоторезисторов, ярким светом. Преимуществом подобных систем является большое число анализируемых параметров, что уменьшает вероятность ошибки.

Аутентификация с помощью автоматического анализа подписи. Известно, что почерк каждого человека строго индивидуален, еще более индивидуальна его подпись. Она становится чрезвычайно стилизованной и со временем приобретает характер условного рефлекса. В настоящее время существуют два принципиально разных способа анализа подписи: визуальное сканирование и исследование динамических характеристик движения руки при выполнении подписи (ускорения, скорости, давления, длительности пауз). Считается, что второй способ предпочтительнее, так как очевидно, что две подписи одного и того же человека не могут быть абсолютно идентичными. С другой стороны, обладая оригиналом подписи, можно научиться повторять ее практически точно.

При втором способе аутентификации предполагается применение специальных измерительных авторучек с датчиками, чувствительными к указанным выше динамическим характеристикам движения. Эти параметры уникальны для каждого человека, их невозможно подделать. Специалисты считают, что система установления подлинности подписи при меньшей стоимости и большей социальной приемлемости не уступает по надежности устройствам, сверяющим отпечатки пальцев.

Аутентификация по характеру голоса. По мнению ряда специалистов, данный метод является наиболее надежным средством аутентификации пользователей. Это направление очень перспективно потому, что для аутентификации могут быть использованы телефонные каналы связи, а алгоритм опознавания может быть реализован в центральной ЭВМ. Устройства аутентификации пользователей по их голосам анализируют спектры голосов, которые сугубо индивидуальны для каждого человека.

Основным выводом, следующим из опыта создания устройств аутентификации, является то, что получение высокой точности опознавания пользователя возможно только при сочетании различных методов. Необходимо отметить, что все рассмотренные методы аутентификации в случае не подтверждения подлинности должны осуществлять временную задержку перед обслужива-

нием следующего запроса. Это необходимо для снижения угрозы подбора идентифицирующих признаков в автоматическом режиме.

Обычно биометрию применяют вместе с другими аутентификаторами, такими, например, как интеллектуальные карты. Иногда биометрическая аутентификация является лишь первым рубежом защиты и служит для активизации интеллектуальных карт, хранящих криптографические секреты; в таком с случае биометрический шаблон хранится на той же карте.

Управление доступом. С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). Логическое управление доступом — это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах — объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа.

Тема логического управления доступом — одна из сложнейших в области ИБ. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные операционные системы могут поддерживать и другие объекты.

Для систем управления реляционными базами данных объект — это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа.

Матрицу доступа, ввиду ее разреженности (большинство клеток — пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Элементами списков могут быть имена групп и шаблоны субъектов, что служит большим подспорьем администратору. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится нечасто.

Списки доступа — исключительно гибкое средство. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек.

Протоколирование и аудит. Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе. Аудит — это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей и администраторов;

- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

При протоколировании события рекомендуется записывать, следующую информацию:

дата и время события;

уникальный идентификатор пользователя — инициатора действия;

тип события;

результат действия (успех или неудача);

источник запроса (например, имя терминала);

имена затронутых объектов (например, открываемых или удаляемых файлов);

описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

Реконструкция последовательности событий позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе.

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или не типичным (согласно принятым критериям).

Задача активного аудита — оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее.

Активность, не соответствующую политике безопасности, целесообразно разделить на атаки, направленные на незаконное получение полномочий, и на действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности.

Атаки нарушают любую осмысленную политику безопасности. Иными словами, активность атакующего является разрушительной независимо от политики. Для описания и выявления атак можно применять универсальные методы, инвариантные относительно политики безопасности, такие как сигнатуры и их обнаружение во входном потоке событий с помощью аппарата экспертных систем.

Сигнатура атаки — это совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию. Простейший пример сигнатуры — "зафиксированы три последовательные неудачные попытки входа в систему с одного терминала", пример ассоциированной реакции — блокирование терминала до прояснения ситуации.

Применительно к средствам активного аудита различают ошибки первого и второго рода: пропуск атак и ложные тревоги, соответственно. Нежелательность ошибок первого рода очевидна; ошибки второго рода не менее неприятны, поскольку отвлекают администратора безопасности от действительно важных дел, косвенно способствуя пропуску атак.

Средства активного аудита могут располагаться на всех линиях обороны информационной системы. На границе контролируемой зоны они могут обнаруживать подозрительную активность в точках подключении к внешним сетям (не только попытки нелегального проникновения, но и действия по "прощупыванию" сервисов безопасности). Важно отметить, что активный аудит, в принципе, способен обеспечить защиту от атак на доступность.

В составе средств активного аудита можно выделить следующие функциональные компоненты:

компоненты генерации регистрационной информации. Они находятся на стыке между средствами активного аудита и контролируемыми объектами;

компоненты хранения сгенерированной регистрационной информации;

компоненты просмотра регистрационной информации. Могут помочь при принятии решения о реагировании на подозрительную активность;

компоненты анализа информации, поступившей от сенсоров. В соответствии с данным выше определением средств активного аудита, выделяют пороговый анализатор, анализатор нарушений

политики безопасности, экспертную систему, выявляющую сигнатуры атак, а также статистический анализатор, обнаруживающий нетипичное поведение;

компоненты хранения информации, участвующей в анализе. Такое хранение необходимо, например, для выявления атак, протяженных во времени;

компоненты принятия решений и реагирования ("решатели"). "Решатель" может получать информацию не только от локальных, но и от внешних анализаторов, проводя так называемый корреляционный анализ распределенных событий;

компоненты хранения информации о контролируемых объектах. Здесь могут храниться как пассивные данные, так и методы, необходимые, например, для извлечения из объекта регистрационной информации или для реагирования;

компоненты, играющие роль организующей оболочки для менеджеров активного аудита, называемые мониторами и объединяющие анализаторы, "решатели", хранилище описаний объектов и интерфейсные компоненты. В число последних входят компоненты интерфейса с другими мониторами, как равноправными, так и входящими в иерархию. Такие интерфейсы необходимы, например, для выявления распределенных, широкомасштабных атак; компоненты интерфейса с администратором безопасности.

Криптографические методы защиты информации.

Криптографические методы защиты информации – это мощное оружие в борьбе за информационную безопасность.

Криптография (от древне-греч. κρυπτος – скрытый и γραφω – пишу) – наука о методах обеспечения конфиденциальности и аутентичности информации.

Криптография необходима для реализации, по крайней мере, трех сервисов безопасности:

- шифрование;
- контроль целостности;
- аутентификация.

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

- защиту конфиденциальности;
- защиту целостности.

Проблемы защиты конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы:

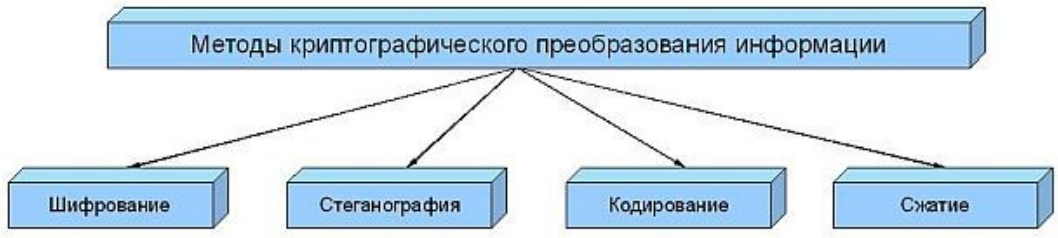


Рис. 1. Классификация методов криптографического преобразования информации

Процесс ***шифрования*** заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Для шифрования информации используются **алгоритм преобразования** и **ключ**. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служит информация, подлежащая зашифрованию, и ключ шифрова-

ния. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемых при реализации алгоритма шифрования. Операнд – это константа, переменная, функция, выражение и другой объект языка программирования, над которым производятся операции.

В отличие от других методов криптографического преобразования информации, методы ***стеганографии*** позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов, т.е. скрываются секретные данные, при этом создаются реалистичные данные, которые невозможно отличить от настоящих. Обработка мультимедийных файлов в информационных системах открыла практически неограниченные возможности перед стеганографией.

Графическая и звуковая информация представляются в числовом виде. Так, в графических объектах наименьший элемент изображения может кодироваться одним байтом. В младшие разряды определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение.

Скрытый файл также может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Содержанием процесса ***кодирование*** информации является замена исходного смысла сообщения (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, знаков. При кодировании и обратном преобразовании используются специальные таблицы или словари. В информационных сетях кодирование исходного сообщения (или сигнала) программно-аппаратными средствами применяется для повышения достоверности передаваемой информации.

Часто кодирование и шифрование ошибочно принимают за одно и тоже, забыв о том, что для восстановления закодированного сообщения, достаточно знать правило замены, в то время как для расшифровки сообщения помимо знания правил шифрования, требуется ключ к шифру.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени передачи данных целесообразно совмещать процесс сжатия и шифрования информации.

Основным видом криптографического преобразования информации в компьютерных сетях является ***шифрование***. Под шифрованием понимается процесс преобразования открытой информации в зашифрованную информацию (шифртекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название зашифрование, а процесс преобразования закрытой информации в открытую – расшифрование.

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров. ***Методом шифрования (шифром)*** называется совокупность обратимых преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, а некоторые используются и до сих пор. Появление компьютеров и компьютерных сетей инициировало процесс разработки новых шифров, учитывающих возможности использования

компьютерной техники как для зашифрования/расшифрования информации, так и для атак на шифр. ***Атака на шифр (криптоанализ, криптоатака)*** – это процесс расшифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

Современные методы шифрования должны отвечать следующим требованиям:

- стойкость шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;
- криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
- шифртекст не должен существенно превосходить по объему исходную информацию;
- ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;
- время шифрования не должно быть большим;
- стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифртексту, при условии, что ему неизвестен ключ.

Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь скрытых слабых мест, которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации – перебор комбинаций ключа и выполнение алгоритма расшифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.

Работа простой криптосистемы проиллюстрирована на рис. 2.

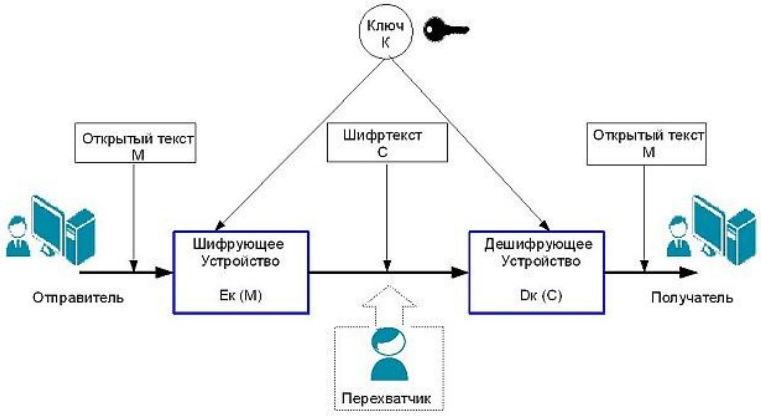


Рис. 2. Обобщённая схема криптографической системы

Преобразование шифрования может быть **симметричным** и **асимметричным** относительно преобразования расшифрования. Это важное свойство определяет два класса криптосистем:

- симметричные (одноключевые) криптосистемы;
- асимметричные (двухключевые) криптосистемы (с открытым ключом).

Симметричное шифрование

Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, в основном используется для обеспечения конфиденциальности данных. Для того чтобы обеспечить конфиденциальность данных, пользователи должны совместно выбрать единый математический алгоритм, который будет использоваться для шифрования и расшифровки данных. Кроме того, им нужно выбрать общий (секретный) ключ, который будет использоваться с принятым ими алгоритмом шифрования/дешифрования, т.е. один и тот же ключ используется и для зашифрования, и для расшифрования (слово "симметричный" означает одинаковый для обеих сторон).

С методом симметричного шифрования связаны следующие проблемы:

• необходимо часто менять секретные ключи, поскольку всегда существует риск их случайного раскрытия (компрометации);

• достаточно сложно обеспечить безопасность секретных ключей при их генерировании, распространении и хранении.

Асимметричное шифрование. Асимметричное шифрование часто называют шифрованием с помощью **открытого ключа**, при котором используются разные, но взаимно дополняющие друг друга ключи и алгоритмы шифрования и расшифровки. Отношение между ключами является математическим – один ключ зашифровывает информацию, а другой ее расшифровывает.

Асимметричное шифрование – система шифрования и/или электронной цифровой подписи (ЭЦП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу, и используется для проверки ЭЦП и для шифрования сообщения. Для генерации цифровой подписи и для расшифрования сообщения используется секретный ключ.

Стеганогра́фия (от греч. στεγανός — скрытый + γράφω — пишу; буквально «тайнопись») — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья или, например, список покупок.

Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её. Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания.

В конце 90-х годов выделилось несколько направлений стеганографии:

1.Классическая стеганография

2.Компьютерная стеганография

3.Цифровая стеганография

Классическая стеганография. Существует версия, что древние шумеры одними из первых использовали стеганографию, так как было найдено множество глиняных клинописных табличек, в которых одна запись покрывалась слоем глины, а на втором слое писалась другая. Однако противники этой версии считают, что это было вовсе не попыткой скрытия информации, а всего лишь практической потребностью. В трудах древнегреческого историка Геродота встречается описание еще двух методов сокрытия информации: на обритую голову раба записывалось необходимое сообщение, а когда его волосы отрастали, он отправлялся к адресату, который вновь брил его голову и считывал доставленное сообщение. Второй способ заключался в следующем: сообщение наносилось на деревянную дощечку, а потом она покрывалась воском, и, тем самым, не вызывала никаких подозрений. Потом воск соскабливался, и сообщение становилось видимым.

Симпатические чернила. Одним из наиболее распространенных методов классической стеганографии является использование симпатических (невидимых) чернил. Текст, записанный такими чернилами, проявляется только при определенных условиях (нагрев, освещение, химический проявитель и т. д.). Изобретенные еще в I веке н. э. Филоном Александрийским, они продолжали использоваться как в средневековье, так и в новейшее время, например, в письмах русских революционеров из тюрем. В советской школьной программе в курсе литературы изучался рассказ о том, как Владимир Ленин писал молоком на бумаге между строк. Молоко проявлялось при нагреве над пламенем. Существуют также чернила с химически нестабильным пигментом. Написанное этими чернилами выглядит как написанное обычной ручкой, но через определенное время нестабильный пигмент разлагается, и от текста не остается и следа. Хотя при использовании обычной шариковой ручки текст можно восстановить по деформации бумаги, этот недостаток можно устранить с помощью мягкого пишущего узла, наподобие фломастера.

Существуют также чернила с химически нестабильным пигментом. Написанное этими чернилами выглядит как написанное обычной ручкой, но через определенное время нестабильный пигмент разлагается, и от текста не остается и следа.

Другой известный многим пример использования стеганографии — акростих. Так, в стихотворении Н. Гумилева «АННА АХМАТОВА»

Ангел лег у края небосклона,
Наклонившись, удивлялся бездне;
Новый мир был синим и беззвездным.
Ад молчал, не слышалось ни стона.
Алой крови робкое биение,
Хрупких рук испуг и содроганье
Миру снов досталось в обладанье
Ангела святое отраженье.
Тесно в мире, пусть живет, мечтая
О любви, о свете и о тени,
В ужасе предвечном открывая
Азбуку своих же откровений

Также существует ряд альтернативных методов сокрытия информации:

• запись на боковой стороне колоды карт, расположенных в условленном порядке;

• запись внутри вареного яйца;

• «жаргонные шифры», где слова имеют другое обусловленное значение;

• трафареты, которые, будучи положенными на текст, оставляют видимыми только значащие буквы;

• узелки на нитках и т. д.

В настоящее время под стеганографией чаще всего понимают скрытие информации в текстовых, графических либо аудиофайлах путём использования специального программного обеспечения.

Комплексная система защиты информации

Вопросы организации защиты информации должны решаться уже на стадии предпроектной разработки ИС. Опыт проектирования систем защиты еще не достаточен. Однако уже можно сделать некоторые обобщения.

Погрешности защиты могут быть в значительной мере устранены, если при проектировании учитывать следующие основные принципы построения системы защиты:

• Простота механизма защиты. Этот принцип общеизвестен, но не всегда глубоко осознается. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты недолжно быть связано со знанием специальных языков или с выполнением трудоемких действий при обычной работе законных пользователей.

• Постоянство защиты. Надежный механизм, реализующий это требование, должен быть постоянно защищен от несанкционированных изменений. Ни одна компьютерная система не может рассматриваться как безопасная, если основные аппаратные и программные механизмы, призванные обеспечивать безопасность, сами являются объектами несанкционированной модификации или видоизменения. • Всеобъемлющий контроль. Этот принцип предполагает необходимость проверки полномочий любого обращения к любому объекту и лежит в основе системы защиты.

• Несекретность проектирования. Механизм защиты должен функционировать достаточно эффективно даже в том случае, если его структура и содержание известны злоумышленнику. Не имеет смысла засекречивать детали реализации системы защиты, предназначенной для широкого использования. Эффективность защиты не должна зависеть от того, насколько опытны потенциальные нарушители. Защита не должна обеспечиваться только секретностью структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно способствовать ее преодолению.

• Идентификация. Каждый объект ИС должен однозначно идентифицироваться. При попытке получения доступа к информации решение о санкционировании его следует принимать на основании данных претендента и определения высшей степени секретности информации, с которой ему разрешается работать. Такие данные об идентификации и полномочиях должны надежно сохраняться и обновляться компьютерной системой для каждого активного участника системы,

выполняющего действия, затрагивающие ее безопасность. Пользователи должны иметь соответствующие полномочия, объекты (файлы) — соответствующий гриф, а система должна контролировать все попытки получения доступа.

• Разделение полномочий. Применение нескольких ключей защиты. Это удобно в тех случаях, когда право на доступ определяется выполнением ряда условий.

• Минимальные полномочия. Для любой программы и любого пользователя должен быть определен минимальный круг полномочий, необходимых для работы.

• Надежность. Система ЗИ должна иметь механизм, который позволил бы оценить обеспечение достаточной надежности функционирования СЗИ (соблюдение правил безопасности, секретности, идентификации и отчетности). Для этого необходимы выверенные и унифицированные аппаратные и программные средства контроля. Целью применения данных механизмов является выполнение определенных задач методом, обеспечивающим безопасность. Максимальная обособленность механизма защиты означает, что защита должна быть отделена от функций управления данными.

Защита памяти. Пакет программ, реализующих защиту, должен размещаться в защищенном поле памяти, чтобы обеспечить системную локализацию попыток проникновения извне. Даже попытка проникновения со стороны программ операционной системы должна автоматически фиксироваться, документироваться и отвергаться, если вызов выполнен некорректно. Удобство для пользователей: схема защиты должна быть в реализации простой, чтобы механизм защиты не создавал для пользователей дополнительных трудностей.

Контроль доступа на основании авторизации пользователя по его физическому ключу и личному PIN-коду. Это обеспечивает защиту от атак неавторизованных пользователей на доступ:

• к ресурсам ПК;

• к областям HD ПК;

• к ресурсам и серверам сети;

• к модулям выполнения авторизации пользователей.

Авторизация пользователя на основании физического ключа позволяет исключить непреднамеренную дискредитацию его прав доступа.

Отчетность. Необходимо защищать контрольные данные от модификации и несанкционированного уничтожения, чтобы обеспечить обнаружение и расследование выявленных фактов нарушения безопасности.

Надежная система должна сохранять сведения о всех событиях, имеющих отношение к безопасности, в контрольных журналах. Кроме того, она должна гарантировать выбор интересующих событий при проведении аудита, чтобы минимизировать стоимость аудита и повысить эффективность анализа.

Наличие программных средств аудита или создание отчетов еще не означает ни усиления безопасности, ни наличия гарантий обнаружения нарушений.

Доступность к исполнению только тех команд операционной системы, которые не могут повредить операционную среду и результат контроля предыдущей аутентификации.

Наличие механизмов защиты от:

• несанкционированного чтения информации;

• модификации хранящейся и циркулирующей в сети информации;

• навязывания информации;

• несанкционированного отказа от авторства переданной информации.

Системный подход к защите информации предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенных для обеспечения безопасности ИС.

Возможность наращивания защиты. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Комплексный подход предполагает согласованное применение разнородных средств защи-

ты информации.

Адекватность — обеспечение необходимого уровня защиты (определяется степенью секретности подлежащей обработке информации) при минимальных издержках на создание механизма защиты и обеспечение его функционирования.

Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и масштаб возможного ущерба были бы приемлемыми (задача анализа риска). Минимизация привилегий в доступе, предоставляемых пользователям, т.е. каждому пользователю должны предоставляться только действительно необходимые ему права по обращению к ресурсам системы и данным. Полнота контроля — обязательный контроль всех обращений к защищаемым данным. Наказуемость нарушений. Наиболее распространенная мера наказания — отказ в доступе к системе. Экономичность механизма — обеспечение минимальности расходов на создание и эксплуатацию механизма.

Принцип системности сводится к тому, что для обеспечения надежной защиты информации в современных ИС должна быть обеспечена надежная и согласованная защита во всех структурных элементах, на всех технологических участках автоматизированной обработки информации и во все время функционирования ИС.

Специализация, как принцип организации защиты, предполагает, что надежный механизм защиты может быть спроектирован и организован лишь профессиональными специалистами по защите информации. Кроме того, для обеспечения эффективного функционирования механизма защиты в состав ИС должны быть включены соответствующие специалисты.

Принцип неформальности означает, что методология проектирования механизма защиты и обеспечения его функционирования в основе своей — неформальна. В настоящее время не существует инженерной (в традиционном понимании этого термина) методики проектирования механизма защиты.

Методики проектирования, разработанные к настоящему времени, содержат комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое их осуществление в общем случае невозможно. Гибкость системы защиты. Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важно это свойство в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

Принцип непрерывности защиты предполагает, что защита информации — это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС.

Разработка системы защиты должна осуществляться параллельно с разработкой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные защищенные информационные системы.

Понятия защиты На формулирование понятия защиты оказывает влияние большое количество разноплановых факторов, основными из которых выступают:

• влияние информации на эффективность принимаемых решений;

• концепции построения и использования защищенных информационных систем;

• техническая оснащенность информационных систем;

• характеристики информационных систем и их компонентов с точки зрения угроз сохранности информации;

• потенциальные возможности злоумышленного воздействия на информацию, ее получение и использование;

• наличие методов и средств защиты информации.

Развитие подходов к защите информации происходит под воздействием перечисленных

факторов, при этом можно условно выделить три периода развития СЗИ:

• первый — относится к тому времени, когда обработка информации осуществлялась по традици Системность подхода Генеральным направлением поиска путей защиты информации является неуклонное повышение системности подхода к самой проблеме защиты информации.

Понятие системности интерпретировалось прежде всего в том смысле, что защита информации заключается не только в создании соответствующих механизмов, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла систем обработки данных при комплексном использовании всех имеющихся средств защиты.

При этом все средства, методы и мероприятия, используемые для защиты информации, непременно и наиболее рационально объединяются в единый целостный механизм — систему защиты, которая должна обеспечивать, говоря военным языком, глубокоэшелонированную оборону, причем не только от злоумышленников, но и от некомпетентных или недостаточно подготовленных пользователей и персонала.

В этой системе должно быть, по крайней мере, четыре защитных пояса: внешний, охватывающий всю территорию, на которой расположены сооружения; пояс сооружений, помещений или устройств системы; пояс компонентов системы (технических средств, программного обеспечения, элементов баз данных) и пояс технологических процессов обработки данных (ввод/ вывод, внутренняя обработка и т.п.).

Основные трудности реализации систем защиты состоят в том, что они должны удовлетворять двум группам противоречивых требований. С одной стороны:

• должна быть обеспечена надежная защита находящейся в системе информации, что в более конкретном выражении формулируется в виде двух обобщенных задач:

• исключение случайной и преднамеренной выдачи информации посторонним лицам и разграничение доступа к устройствам;

• и ресурсам системы всех пользователей, администрации и обслуживающего персонала.

С другой стороны, системы защиты не должны создавать заметных неудобств в процессе работы с использованием ресурсов системы. В частности должны быть гарантированы:

• полная свобода доступа каждого пользователя и независимость его работы в пределах предоставленных ему прав и полномочий;

• удобство работы с информацией для групп взаимосвязанных пользователей;

• возможности пользователям допускать друг друга к своей информации.

Основные правила защиты, которыми рекомендуют руководствоваться специалисты при организации работ по защите информации, сводятся к следующему:

1. Обеспечение безопасности информации есть непрерывный процесс, состоящий в систематическом контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.

2. Безопасность информации в системе обработки данных может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты.

3. Никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты

4. Никакую систему защиты нельзя считать абсолютно надежной, следует исходить из того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

С самых первых этапов, т.е. с той поры, когда проблема защиты информации в системах обработки данных стала рассматриваться как самостоятельная, основными средствами, используемыми для защиты, были технические и программные.

Техническими названы такие средства, которые реализуются в виде электрических, электромеханических, электронных устройств. Всю совокупность технических средств принято делить на аппаратные и физические. Под аппаратными средствами защиты понимают устройства, внедряемые непосредственно в аппаратуру обработки данных, или устройства, которые сопрягаются с ней по стандартному интерфейсу. Наиболее известные аппаратные средства, используемые на

первом этапе — это схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры (например, регистры границ поля ЗУ) и т.п.

Физическими средствами названы такие, которые реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения, замки на дверях, ре шетки на окнах и т.п.).

Программные средства защиты, как известно, об разуют программы специально предназначенные для выполнения функций, связанных с защитой информации. Первоначально программные механизмы защиты включались в состав операционных систем или систем управления базами данных. Этим, видимо, и объясняется, что практически все без исключения операционные системы содержат механизмы защиты информации от несанкционированного доступа, а именно:

• динамическое распределение ресурсов вычисли тельной системы и запрещение задачам пользователей использовать чужие ресурсы;

• разграничение доступа пользователей к ресурсам системы по паролям;

• разграничение доступа к полям оперативной и долговременной памяти по ключам защиты;

• защита таблицы паролей с помощью так называемого главного пароля.

Защищенная ИС и система защиты информации Многие специалисты считают, что точный ответ на вопрос, что же такое "защищенная информационная система", пока не найден.

Существуют следующие представления защищенности ИС:

• это совокупность средств и технологических приемов, обеспечивающих защиту компонентов ИС;

• это минимизация риска, которому могут быть подвергнуты компоненты и ресурсы ИС;

• это комплекс процедурных, логических и физических мер, направленных на предотвращение угроз информации и компонентам ИС.

Защищенной будем называть ИС, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов этой ИС. При этом механизмы выполнения указанных правил чаще всего реализуются в виде системы защиты информации.

Следовательно, под СЗИ будем понимать совокупность механизмов защиты, реализующих установленные правила, удовлетворяющие указанным требованиям. Таким образом, список угроз информации определяет основу для формирования требований к защите. Когда такие требования известны, могут быть определены соответствующие правила обеспечения защиты. Эти правила, в свою очередь, определяют необходимые функции и средства защиты, объединенные в комплексную СЗИ. Можно утверждать, что чем полнее будет список требований к защите и соответствующих правил защиты, тем эффективнее будет СЗИ для данной ИС. Для того чтобы построить защищенную ИС, целесообразно провести анализ угроз информации, составить перечень требований к защите, сформулировать правила организации непосредственной защиты и реализовать их выполнение путем создания комплексной СЗИ, которая представляет собой действующие в единой совокупности законодательные, организационные, технические и другие способы и средства, обеспечивающие защиту важной информации от всех выявленных угроз и возможных каналов утечки.

Как обеспечить сохранность информации? Как же обеспечить сохранность своей информации? Ведь многообразие вариантов построения информационных систем порождает необходимость создания раз личных систем защиты, учитывающих индивидуальные особенности каждой из них. Вместе с тем, в настоящее время разработано и применяется большое количество технологий, способов и средств защиты информации, которые необходимо проанализировать и использовать в информационных системах уже сегодня. Это позволит резко сократить утечку сведений конфиденциального характера.

Руководителям следует помнить, что закон Мерфи актуален и для проблем защиты информации. Напомним его содержание:

Если какая-нибудь неприятность может случиться, она случается. Следствия.

1. Все не так легко, как кажется.

2. Всякая работа требует больше времени, чем вы думаете.

3. Из всех неприятностей произойдет именно та, ущерб от которой больше.

4. Если четыре причины возможных неприятностей заранее устранены, то всегда найдется пятая.

5. Предоставленные самим себе, события имеют тенденцию развиваться от плохого к худшему.

6. Как только вы принимаетесь делать какую-то работу, находится другая, которую надо сделать еще раньше.

7. Всякое решение плодит новые проблемы.

Приступая к работе по созданию защищенной ИС, желательно в собственном представлении создать об раз Вашей ИС в любом удобном для простого понимания виде. Попробуйте включить фантазию в этот процесс. Прежде чем начать разговор о возможных путях организации зашиты информации (ЗИ), необходимо определиться, имеется ли у Вас информация, которую нельзя не защищать; это важно, поскольку, как правило, ЗИ потребует дополнительных средств и достаточно больших. СЗИ — довольно дорогостоящее удовольствие (а чаще необходимость).

И если после долгих колебаний и споров решено, что в ИС имеет место информация, которую необходимо защищать, не расстраивайтесь. Далее необходимо определить конкретные сведения, подлежащие защите, для чего и от кого их защищать, а так же степень надежности такой защиты — проделать это не сложно.

После этого следует выявить потенциальные угрозы и наиболее вероятные каналы утечки информации для конкретных условий. Их может оказаться достаточно много, но не стоит огорчаться, так как злоумышленник не будет их использовать все сразу.

Следующим шагом будет выбор из множества предлагаемых вариантов таких методов, мероприятий и средств, которые можно было бы использовать конкретно в Вашей ИС. После того как удалось найти конкретные варианты организационных и технических решений, необходимо подсчитать затраты на их реализацию. Вот здесь можно и огорчиться.

Сомнения и чувство досады, возникающие в такие моменты — это вполне нормальное явление. Часто при этом всплывают воспоминания о том, как спокойно жилось, пока проблемы защиты ин формации не были Вам знакомы. Но рано или поздно наступает момент, когда становится ясно: как бы мы этого не хотели, а придется выложить дополнительные средства на организацию защиты своих данных. Было бы неплохо, чтобы такая мысль пришла пораньше, поскольку построить систему защиты информации для готовой (законченной) информационной системы можно лишь путем введения целого ряда ограничений, а это, естественно, снижает эффективность функционирования информационной системы в целом.

Лучше всего анализировать опасности еще на стадии проектирования рабочего места, локальной сети или всей системы, чтобы сразу определить потенциальные потери и установить требования к мерам обеспечения безопасности. Выбор защитных и контрольных мероприятий на этой ранней стадии требует гораздо меньших затрат, чем выполнение подобной работы с эксплуатируемой компьютерной системой. Чаще всего бывает достаточно анализа возможных опасностей, чтобы осознать проблемы, которые могут проявиться во время работы.

Недаром эксперты по безопасности компьютерных систем часто подчеркивают, что проблемы ЗИ в значительной степени являются социальными, и если эти проблемы загонять внутрь, они могут "выйти боком". Все усилия и средства по защите информации должны быть объединены в стройную систему защиты информации, работающую по принципу: "копейка рубль бережет". Современные популярные и доступные широкому кругу пользователей персональные компьютеры в действительности не обеспечивают безопасность информации, поскольку любой, кто имеет доступ к компьютеру, может изменять, читать или копировать данные.

Изначально ПК были созданы для решения бытовых и офисных задач и не предназначались для обработки секретной или конфиденциальной информации. Несколько позднее на базе таких ПК появились локальные сети, а вместе с ними — и "головная боль" от проблем защиты информа-

ции. Конечно, решить все эти проблемы непросто. Но, как говорится, вместо того, чтобы хвататься за голову, необходимо просто взяться за ум. Создание СЗИ можно сравнить с пошивом костюма. При наличии обязательных составляющих (брюки, пиджак, рукава, воротник...) имеется множество фасонов (вариантов покроя), при этом необходимо учитывать индивидуальные особенности каждого заказчика (пропорции тела, вкусы, привычки...).

В итоге все стремятся получить удобную, практичную, качественную, красивую, современную вещь. Серьезная работа по практическому использованию информационных технологий началась сравнительно недавно.

Широкий выбор разнообразного аппаратного и программного обеспечения позволяет построить ИС под свои конкретные задачи. Но, как это часто бывает, наблюдается существенный разрыв между тем, что мы имеем в своем распоряжении и тем, что мы можем из этого извлечь... Иначе говоря, компьютер можно использовать не только в качестве неплохой пишущей машинки. Давно известно, что рыть траншею и прокладывать кабель (или трубы) желательно до того, как в этом месте положат асфальт.

Так и СЗИ целесообразно строить одновременно с ИС, начиная с этапа проектирования. А можно ли сэкономить на своей информационной безопасности? Да, можно! Но стоить это будет дороже!

Основные правила, которыми рекомендуют руководствоваться специалисты при организации работ по защите информации, сводятся к следующему:

1. Обеспечение безопасности информации есть непрерывный процесс, состоящий в систематическом контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.

2. Безопасность информации в системе обработки данных может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств за щиты.

3. Никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты.

4. Никакую систему защиты нельзя считать абсолютно надежной, следует исходить из того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

Существуют следующие представления защищенности ИС:

• защищенность это совокупность средств и технологических приемов, обеспечивающих защиту компонентов ИС;

• защищенность это минимизация риска, которому могут быть подвергнуты компоненты и ресурсы ИС;

• защищенность это комплекс процедурных, логических и физических мер, направленных на предотвращение угроз информации и компонентам ИС.

Защищенной ИС будем называть ИС, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов этой ИС.

При этом механизмы выполнения указанных правил чаще всего реализуются в виде системы защиты информации. Следовательно, под СЗИ будем понимать совокупность механизмов защиты, реализующих установленные правила, удовлетворяющие указанным требованиям.

Прежде всего, необходима полная идентификация пользователей, терминалов, программ, а также основных процессов и процедур, желательно до уровня записи или элемента. Кроме того следует ограничить доступ к информации, используя совокупность следующих способов:

• иерархическая классификация доступа,

• классификация информации по важности и месту ее возникновения,

• указание ограничений к информационным объектам, например пользователь может осуществлять только чтение файла без права записи в него,

• определение программ и процедур, предоставленных только конкретным пользователям.

Система защиты должна гарантировать, что любое движение данных идентифицируется,

авторизуется, обнаруживается и документируется. Обычно формулируются общие требования к следующим характеристикам:

• способам построения СЗИ либо ее отдельных компонент (к программному, программно-аппаратному, аппаратному);

• архитектуре СВТ и ИС (к классу и минимальной конфигурации ЭВМ, операционной среде, ориентации на ту или иную программную и аппаратную платформы, архитектуре интерфейса);

• применению стратегии защиты;

• затратам ресурсов на обеспечение СЗИ (к объемам дисковой памяти для программной версии и оперативной памяти для ее резидентной части, затратам производительности вычислительной системы на решение задач защиты);

• надежности функционирования СЗИ (к количественным значениям показателей надежности во всех режимах функционирования ИС и при воздействии внешних разрушающих факторов, к критериям отказов);

• количеству степеней секретности информации, поддерживаемых СЗИ;

• обеспечению скорости обмена информацией в ИС, в том числе с учетом используемых криптографических преобразований;

• количеству поддерживаемых СЗИ уровней полномочий;

• возможности СЗИ обслуживать определенное количество пользователей;

• продолжительности процедуры генерации программной версии СЗИ;

• продолжительности процедуры подготовки СЗИ к работе после подачи питания на компоненты ИС;

• возможности СЗИ реагировать на попытки несанкционированного доступа, либо на "опасные ситуации";

• наличию и обеспечению автоматизированного рабочего места администратора защиты информации в ИС;

• составу используемого программного и лингвистического обеспечения, к его совместимости с другими программными платформами, к возможности модификации и т.п.;

• используемым закупаемым компонентам СЗИ (наличие лицензии, сертификата и т.п.).

Рис. 1. Совокупность требований к СЗИ

В общем случае СЗИ целесообразно условно разделить на подсистемы:

• управления доступом к ресурсам ИС (включает также функции управления системой защиты в целом);

• регистрации и учета действий пользователей (процессов);

• криптографическую;

• обеспечения целостности информационных ресурсов и конфигурации ИС.

Для каждой из них определяются требования в виде:

• перечня обеспечиваемых подсистемой функций защиты;

• основных характеристик этих функций;

• перечня средств, реализующих эти функции.

Подсистема управления доступом должна обеспечивать:

• идентификацию, аутентификацию и контроль за доступом пользователей (процессов) к системе, терминалам, узлам сети, каналам связи, внешним устройствам, программам, каталогам, файлам, записям и т.д.;

• управление потоками информации;

• очистку освобождаемых областей оперативной памяти и внешних накопителей.

Подсистема регистрации и учета выполняет:

• регистрацию и учет: доступа в ИС, выдачи выходных документов, запуска программ и процессов, доступа к защищаемым файлам; передачу данных по линиям и каналам связи;

• регистрацию изменения полномочий доступа, создание объектов доступа, подлежащих защите;

• учет носителей информации;

• оповещение о попытках нарушения защиты.

Криптографическая подсистема предусматривает:

• шифрование конфиденциальной информации.

• шифрование информации, принадлежащей разным субъектам доступа (группам субъектов), с использованием разных ключей.

• использование аттестованных (сертифицированных) криптографических средств.

Подсистема обеспечения целостности осуществляет:

• обеспечение целостности программных средств и обрабатываемой информации,

• физическую охрану средств вычислительной техники и носителей информации,

• наличие администратора (службы) защиты информации в ИС,

• периодическое тестирование СЗИ,

• наличие средств восстановления СЗИ,

• использование сертифицированных средств защиты,

Контроль за целостностью:

• программных средств защиты информации при загрузке операционной среды,

• операционной среды перед выполнением процессов,

• функционального ПО и данных,

• конфигурации ИС,

• оперативное восстановление функций СЗИ после сбоев,

• тестирование средств защиты информации,

• обнаружение и блокирование распространения вирусов,

• резервное копирование программного обеспечения и данных,

• контроль доступа к СВТ, дающий уверенность в том, что только авторизованный пользователь использует имеющиеся рабочие программы и информацию,

• контроль действий с персональной авторизацией, запрещающий операции, которые делают операционную среду уязвимой,

• защиту программного обеспечения, исключающую повреждение инсталлированных программ,

• использование только лицензионного программного продукта с целью обеспечения защиты

от встроенных модулей разрушения информационной среды и дискредитации систем защиты;

• защиту коммуникаций для обеспечения недоступности передаваемой информации.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ

Лабораторная работа 1. Использование антивирусных программ.

Цель: Целью выполнения лабораторной работы является изучение принципов работы антивирусных средств и их использования для зашиты от вредоносных программных воздействий.

Задание

1. Посмотрите, какие антивирусные программы установлены на Вашем ПК.
2. Откройте антивирусную программу и изучите окно программы.
3. Почитайте информацию на вкладках: Состояние защиты, Обновление, Настройка, Служебные программы, Справка и поддержка.
4. Посмотрите на вкладке Настройка, все ли опции включены: Защита в режиме реального времени, Защита электронной почты, Защита доступа в Интернет.
5. Включите вкладку Сканирование ПК. Выберите выборочное сканирование. Просканируйте диск локальный D.
6. Пока идёт сканирование, изучите содержимое вкладки Служебные программы. Какие файлы были помещены на карантин?
7. После окончания сканирования локального диска просканируйте свою дискету.
8. В разделе Справочной системы программы найдите информацию о том, какие *три уровня очистки* поддерживает программа.
9. Изучите раздел справки *Введение в интерфейс пользователя*.
10. Изучите раздел справки *Предупреждения и уведомления*.

Контрольные вопросы.

1. Какие разновидности вирусов Вы знаете?
2. Как вирусы классифицируются по среде обитания?
3. Как вирусы классифицируются по степени вредного воздействия?
4. Какие виды вредоносных программ Вы знаете?
5. Как вирусы маскируются?
6. Какие действия могут выполнять антивирусные программы?
7. Какие три задачи должна выполнять антивирусная программа?
8. Как обеспечить безопасность своей информации?

Лабораторная работа 2. Изучение традиционных симметричных криптосистем. Шифры перестановок.

Цель: Целью выполнения лабораторной работы является изучение традиционных симметричных криптосистем.

Задание.

1. Зашифровать 81 символ текста методом одиночной перестановки по ключу. Нумерацию символов ключевого слова проводить по табл. 1. Знаки препинания и пробелы не учитывать.

2. Поменяться с соседом зашифрованными текстами и ключами. Расшифровать текст.

Шифрующие таблицы

В эпоху Возрождения (с конца XIV в.) начала возрождаться и криптография. Наряду с традиционными вариантами применения криптографии в политике, дипломатии и военном деле появляются и другие - защита интеллектуальной собственности от инквизиции или от злоумышленников. В разработанных шифрах того времени применяются шифрующие таблицы, которые, в сущности, задают правила перестановки букв в сообщении.

В качестве ключа в шифрующих таблицах используются:

размер таблицы;

слово или фраза, задающие перестановку;

особенности структуры таблицы.

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы. Этот метод шифрования сходен с шифром "скитала". Например, сообщение:

"ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ"

записывается в таблицу поочередно по столбцам. Результат заполнения таблицы из 5 строк и 7 столбцов показан на рис. 1.

Т	**Н**	**П**	**В**	**Е**	**Г**	**Л**
Е	**А**	**Р**	**А**	**Д**	**О**	**Н**
Р	**Т**	**И**	**Е**	**Ь**	**В**	**О**
М	**О**	**Б**	**Т**	**М**	**П**	**Ч**
И	**Р**	**Ы**	**С**	**О**	**О**	**Ь**

Рис. 1. Заполнение таблицы из 5 строк и 7 столбцов

После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам. Если шифртекст записывать группами по пять букв, получается такое шифрованное сообщение:

ТНПВЕ ГЛЕАР АДОНР ТИЕЬВ ОМОБТ МПЧИР ЫСООЬ

Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Следует заметить, что объединение букв шифртекста в 5-буквенные группы не входит в ключ шифра и осуществляется для удобства записи несмыслового текста. При расшифровке действия выполняют в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый "одиночная перестановка по ключу". Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Применим в качестве ключа, например, слово:

"ПЕЛИКАН",

а текст сообщения возьмем из предыдущего примера. На рис. 2 показаны две таблицы, заполненные текстом сообщения и ключевым словом, при этом левая таблица соответствует заполнению до перестановки, а правая - после перестановки.

КЛЮЧ

→

П	**Е**	**Л**	**И**	**К**	**А**	**Н**
7	**2**	**5**	**3**	**4**	**1**	**6**
Т	**Н**	**П**	**В**	**Е**	**Г**	**Л**
Е	**А**	**Р**	**А**	**Д**	**О**	**Н**
Р	**Т**	**И**	**Е**	**Ь**	**В**	**О**
М	**О**	**Б**	**Т**	**М**	**П**	**Ч**
И	**Р**	**Ы**	**С**	**О**	**О**	**Ь**

А	**Е**	**И**	**К**	**Л**	**Н**	**П**
1	**2**	**3**	**4**	**5**	**6**	**7**
Г	**Н**	**В**	**Е**	**П**	**Л**	**Т**
О	**А**	**А**	**Д**	**Р**	**Н**	**Е**
В	**Т**	**Е**	**Ь**	**И**	**О**	**Р**
П	**О**	**Т**	**М**	**Б**	**Ч**	**М**
О	**Р**	**С**	**О**	**Ы**	**Ь**	**И**

До перестановки После перестановки

Рис 2. Таблицы, заполненные ключевым словом и текстом сообщения

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если бы в ключе встретились одинаковые буквы, они бы были понумерованы слева направо. В правой таблице столбцы переставлены в соответствии с упорядоченными номерами букв ключа.

При считывании содержимого правой таблицы по строкам и записи шифртекста группами по пять букв получим шифрованное сообщение:

ГНВЕП ЛТОАА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЫЬИ

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется **двойной перестановкой**. В этом случае перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в

таблицу записывается текст сообщения, потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок должен быть обратным.

Таблица 1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Р	С	Т	У	Ф	К	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я

Номер варианта	Текст	Ключевое слов
1.	ДУМАЕТСЯ, ЧТО КАЖДОМУ ЧИТАТЕЛЮ ДАННОГО ПОСОБИЯ ДОВОДИЛОСЬ СДАВАТЬ КАКИЕ-ЛИБО ЭКЗАМЕНЫ И ВЫ ВСЕ БОЛЕЕ ИЛИ МЕНЕЕ ПРЕДСТАВЛЯЕТЕ СЕБЕ, ЧТО ЭТО ТАКОЕ.	ДИПЛОМАНТ
2.	ТЕМ НЕ МЕНЕЕ, ДЛЯ РАЗРАБОТКИ ПОДЛИННО НАУЧНОГО ПОДХОДА НЕОБХОДИМО ТОЧНОЕ ОПРЕДЕЛЕНИЕ ИЗУЧАЕМОГО ЯВЛЕНИЯ.	КИМБЕРЛИТ
3.	БУДЬ Я МИНИСТРОМ ОБРАЗОВАНИЯ, ВО ВСЕХ ВУЗАХ ВВЕЛ БЫ В ОБЯЗАТЕЛЬНОМ ПОРЯДКЕ ИЗУЧЕНИЕ МЕТОДОВ ОТЛЫНИВАНИЯ, ТЕХНОЛОГИИ ИЗГОТОВЛЕНИЯ ШПАРГАЛОК И ИСКУССТВА ЛИТЬ ВОДУ, ПРИЧЕМ С ОБЯЗАТЕЛЬНЫМ ЭКЗАМЕНОМ	КРОНШТЕЙН
4.	ВООБРАЗИТЕ ОТРАДНУЮ КАРТИНУ: СТУДЕНТ, ИЗГОТОВЛЯЮЩИЙ "ШПОРЫ" НА ЭКЗАМЕН ПО ШПАРГАЛКОВЕДЕНИЮ	КРУПОЗНЫЙ
5.	И ДЕЙСТВИТЕЛЬНО, В ПРОЦЕССЕ ЭКЗАМЕНА ИСПЫТЫВАЮТСЯ САМЫЕ РАЗНООБРАЗНЫЕ КАЧЕСТВА СТУДЕНТА - ОТ ОРАТОРСКОГО МАСТЕРСТВА ДО ИСКУССТВА ПАНТОМИМЫ	МАССАЖИСТ
6.	СРАЗУ ХОЧУ ОТМЕТИТЬ МОЕ ПРИНЦИПИАЛЬНОЕ НЕСОГЛАСИЕ С ОБЩЕПРИНЯТЫМИ ТРАКТОВКАМИ, В КОТОРЫХ СТУДЕНТ ВЫСТУПАЕТ ПАССИВНЫМ ОБЪЕКТОМ, НАД КОТОРЫМ ЭКЗАМЕНАТОРЫ ПРОДЕЛЫВАЮТ КАКИЕ-ЛИБО ТОЛЬКО ИМ ПОДКОНТРОЛЬНЫЕ ДЕЙСТВИЯ	КРУПЧАТКА
7.	НАПРОТИВ, ИДЕАЛЬНЫЙ ЭКЗАМЕНАТОР ВЫПОЛНЯЕТ РОЛЬ БЕСПРИСТРАСТНОГО ИЗМЕРИТЕЛЯ УРОВНЯ ЗНАНИЙ СТУДЕНТА	ЛАНДКАРТА
8.	СЛЕДУЕТ ПРИЗНАТЬ, ЧТО ТАКОЙ ТИП В ПРИРОДЕ НЕ ВСТРЕЧАЕТСЯ. ЭКЗАМЕНАТОР МОЖЕТ БЫТЬ НАСТРОЕН ПО ОТНОШЕНИЮ К СТУДЕНТУ ПОЛОЖИТЕЛЬНО ИЛИ ОТРИЦАТЕЛЬНО, НО ВЕДЬ ТАКИМ ЕГО ДЕЛАЕТ САМ СТУДЕНТ	ЛАМАРКИЗМ
9.	СЛЕДОВАТЕЛЬНО, ЭКЗАМЕН НАЧИНАЕТСЯ НЕ ТОГДА, КОГДА ВАША ДРОЖАЩАЯ РУКА ТЯНЕТСЯ ЗА БИЛЕТОМ, А ЕЩЕ ПРИ ПЕРВОЙ ВСТРЕЧЕ СТУДЕНТА С БУДУЩИМ ЭКЗАМЕНАТОРОМ	ЛАКРИНЧИК
10.	ЭКЗАМЕН МОЖНО ОПРЕДЕЛИТЬ КАК СОВОКУПНОСТЬ ДЕЙСТВИЙ СТУДЕНТА, НАПРАВЛЕННЫХ НА ТО, ЧТОБЫ ЭКЗАМЕНАТОР ПОСЧИТАЛ ЕГО ДОСТОЙНЫМ КАК МОЖНО БОЛЕЕ ВЫСОКОЙ ОЦЕНКИ	ОРТОПЕДИЯ
11.	ДО СИХ ПОР Я ЧАСТО ВСПОМИНАЮ СВОЙ ПОСЛЕДНИЙ ШКОЛЬНЫЙ ЭКЗАМЕН ПО ФИЗИКЕ. ПРИНИМАЛА ЕГО УЧИТЕЛЬНИЦА, ТВЕРДО УВЕРЕННАЯ В МОИХ ГЛУБОКИХ ПОЗНАНИЯХ В ЭТОЙ ОБЛАСТИ	СЕРПОВИЩЕ
12.	ВОЛЕЙ СУДЕБ МНЕ ПРИШЛОСЬ ОТВЕЧАТЬ НА ВОПРОС О ФИЛОСОФСКИХ КОНЦЕПЦИЯХ, ПРИМЕНИМЫХ В ФИЗИКЕ. ОБ ЭТОМ Я НЕ ЗНАЛ АБСОЛЮТНО НИЧЕГО	СУСПЕНЗИЯ
13.	ДЛЯ ТОГО, ЧТОБЫ РАССМАТРИВАТЬ В ДАЛЬНЕЙШЕМ ВОПРОСЫ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ, НЕОБХОДИМО НАПОМНИТЬ ОСНОВНЫЕ ПОНЯТИЯ, КОТОРЫМИ ОПЕРИРУЕТ ТЕОРИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ	ОБРАБОТКА
14.	ОСНОВНОЙ ОСОБЕННОСТЬЮ ЛЮБОЙ СЕТЕВОЙ СИСТЕМЫ ЯВЛЯЕТСЯ ТО, ЧТО ЕЕ КОМПОНЕНТЫ РАСПРЕДЕЛЕНЫ В ПРОСТРАНСТВЕ И СВЯЗЬ МЕЖДУ НИМИ ФИЗИЧЕСКИ ОСУЩЕСТВЛЯЕТСЯ ПРИ ПОМОЩИ СЕТЕВЫХ СОЕДИНЕНИЙ	ОПАСНОСТЬ

Номер варианта	Текст	Ключевое слов
15.	УГРОЗА БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СИСТЕМЫ - ЭТО ПОТЕНЦИАЛЬНО ВОЗМОЖНОЕ ПРОИСШЕСТВИЕ, НЕВАЖНО, ПРЕДНАМЕРЕННОЕ ИЛИ НЕТ, КОТОРОЕ МОЖЕТ ОКАЗАТЬ НЕЖЕЛАТЕЛЬНОЕ ВОЗДЕЙСТВИЕ НА САМУ СИСТЕМУ, А ТАКЖЕ НА ИНФОРМАЦИЮ, ХРАНЯЩУЮСЯ В НЕЙ	СОВЕТСКИЙ
16.	УЯЗВИМОСТЬ КОМПЬЮТЕРНОЙ СИСТЕМЫ - ЭТО НЕКАЯ ЕЕ НЕУДАЧНАЯ ХАРАКТЕРИСТИКА, КОТОРАЯ ДЕЛАЕТ ВОЗМОЖНЫМ ВОЗНИКНОВЕНИЕ УГРОЗЫ	ОТНОШЕНИЕ
17.	УГРОЗА ОТКАЗА В ОБСЛУЖИВАНИИ ВОЗНИКАЕТ ВСЯКИЙ РАЗ, КОГДА В РЕЗУЛЬТАТЕ НЕКОТОРЫХ ДЕЙСТВИЙ БЛОКИРУЕТСЯ ДОСТУП К НЕКОТОРОМУ РЕСУРСУ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ	ИЕРУСАЛИМ
18.	АТАКА НА КОМПЬЮТЕРНУЮ СИСТЕМУ - ЭТО ДЕЙСТВИЕ, ПРЕДПРИНИМАЕМОЕ ЗЛОУМЫШЛЕННИКОМ, КОТОРОЕ ЗАКЛЮЧАЕТСЯ В ПОИСКЕ И ИСПОЛЬЗОВАНИИ ТОЙ ИЛИ ИНОЙ УЯЗВИМОСТИ	НАЧАЛЬНИК
19.	ИССЛЕДОВАТЕЛИ ОБЫЧНО ВЫДЕЛЯЮТ ТРИ ОСНОВНЫХ ВИДА УГРОЗ БЕЗОПАСНОСТИ - ЭТО УГРОЗЫ РАСКРЫТИЯ, ЦЕЛОСТНОСТИ И ОТКАЗА В ОБСЛУЖИВАНИИ	ПОКОЛЕНИЕ
20.	В ТЕРМИНАХ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ УГРОЗА РАСКРЫТИЯ ИМЕЕТ МЕСТО ВСЯКИЙ РАЗ, КОГДА ПОЛУЧЕН ДОСТУП К НЕКОТОРОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ХРАНЯЩЕЙСЯ В ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ ИЛИ ПЕРЕДАВАЕМОЙ ОТ ОДНОЙ СИСТЕМЫ К ДРУГОЙ	КОНЦЕПЦИЯ

Лабораторная работа 3. Изучение традиционных симметричных криптосистем. Шифры замены.

Цель: Целью выполнения лабораторной работы является изучение традиционных симметричных криптосистем.

Задание.

1. Зашифровать текст при помощи таблицы Вижинера, используя ключевое слово.
2. Поменяться с соседом зашифрованными текстами и ключами. Расшифровать текст.

ШИФРЫ ЗАМЕНЫ

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста. Часто шифры простой замены называют шифрами одноалфавитной подстановки.

Полибианский квадрат.

Одним из первых шифров простой замены считается так называемый *полибианский квадрат.* За два века до нашей эры греческий писатель и историк Полибий изобрел для целей шифрования квадратную таблицу размером 5x5, заполненную буквами греческого алфавита в случайном порядке (рис. 1).

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	x
χ	ν		φ	ι

Рис. 1. Полибианский квадрат, заполненный случайным образом 24 буквами греческого алфавита и пробелом

При шифровании в этом полибианском квадрате находили очередную букву открытого текста и записывали в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста

оказывалась в нижней строке таблицы, то для шифртекста брали самую верхнюю букву из того же столбца. Например, для слова:

ταυροσ

получается шифртекст

χφδμτξ

Концепция полибианского квадрата оказалась плодотворной и нашла применение в криптосистемах последующего времени.

Система шифрования Цезаря.

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Свое название он получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном (около 50 г. до н.э.).

При шифровании исходного текста каждая буква заменялась на другую букву того же алфавита по следующему правилу. Заменяющая буква определялась путем смещения по алфавиту от исходной буквы на **К** букв. При достижении конца алфавита выполнялся циклический переход к его началу. Цезарь использовал шифр замены при смещении **К = 3**. Такой шифр замены можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифртекста. Совокупность возможных подстановок для **К = 3** показана в табл. 1.

Таблица 1

Одноалфавитные подстановки (К = 3, m = 26).

A	→	**D**	**J**	→	**M**	**S**	→	**V**
B	→	**E**	**K**	→	**N**	**T**	→	**W**
C	→	**F**	**L**	→	**O**	**U**	→	**X**
D	→	**G**	**M**	→	**P**	**V**	→	**Y**
E	→	**H**	**N**	→	**Q**	**W**	→	**Z**
F	→	**I**	**O**	→	**R**	**X**	→	**A**
G	→	**J**	**P**	→	**S**	**Y**	→	**B**
H	→	**K**	**Q**	→	**T**	**Z**	→	**C**
I	→	**L**	**R**	→	**U**			

Например, послание Цезаря

"VENI VIDI VICI"

(в переводе на русский означает "Пришел, Увидел, Победил"), направленное его другу Аминтию после победы над понтийским царем Фарнаком, сыном Митридата, выглядело бы в зашифрован ном виде так:

YHQL YLGL YLFL

Достоинством системы шифрования Цезаря является простота шифрования и расшифровки. К недостаткам системы Цезаря следует отнести следующие:

подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного открытого текста;

сохраняется алфавитный порядок в последовательности заменяющих букв; при изменении значения **К** изменяются только начальные позиции такой последовательности;

число возможных ключей **К** мало;

шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифртексте.

Криптоаналитическая атака против системы одноалфавитной замены начинается с подсчета частот появления символов: определяется число появлений каждой буквы в шифртексте. Затем полученное распределение частот букв в шифртексте сравнивается с распределением частот букв в алфавите исходных сообщений, например, в английском. Буква с наивысшей частотой по явления в шифртексте заменяется на букву с наивысшей частотой появления в английском языке и т.д. Вероятность успешного вскрытия системы шифрования повышается с увеличением длины шифртекста.

Концепция, заложенная в систему шифрования Цезаря, оказалась весьма плодотворной, о чем свидетельствуют ее многочисленные модификации.

Шифрующие таблицы Трисемуса

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием "Полиграфия". В ней он впервые систематизировал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

Поскольку ключевое слово или фразу легко хранить в памяти, то такой подход упрощал процессы шифрования и расшифровки.

Б	***А***	Н	***Д***	***Е***	Р	О	Л
Ь	В	Г	Ж	З	И	И	К
М	П	С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ы	Ъ	Э	Ю	Я

Рис. 2. Шифрующая таблица с ключевым словом "БАНДЕРОЛЬ"

Как и в случае полибианского квадрата, при шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца. Например, при шифровании с помощью этой таблицы сообщения:

"ВЫЛЕТАЕМПЯТОГО"

получаем шифртекст:

"ПДКЗЫВЗЧШЛЫЙСЙ".

Такие табличные шифры называются монограммными, так как шифрование выполняется по одной букве. Трисемус первым заметил, что шифрующие таблицы позволяют шифровать сразу по две буквы. Такие шифры называются ***биграммными.***

Шифры сложной замены

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свои шифр простой замены. Многоалфавитная подстановка последовательно и циклически меняет используемые алфавиты.

Шифр Гронсфельда

Этот шифр сложной замены представляет собой модификацию шифра Цезаря числовым ключом. Под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно как в шифре Цезаря, но отсчитывают по алфавиту не третью букву (как в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа **е** (основания натуральных логарифмов – 2718), получаем для исходного сообщения **"ВОСТОЧНЫЙ ЭКСПРЕСС"** следующий шифртекст:

Сообщение	**В**	**О**	**С**	**Т**	**О**	**Ч**	**Н**	**Ы**	**Й**	**Э**	**К**	**С**	**П**	**Р**	**Е**	**С**	**С**
Ключ	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**
Шифртекст	**Д**	**Х**	**Т**	**Ь**	**Р**	**Ю**	**О**	**Г**	**Л**	**Д**	**Л**	**Щ**	**С**	**Ч**	**Ж**	**Щ**	**У**

Чтобы зашифровать первую букву сообщения (В), используя первую цифру ключа 2, нужно отсчитать вторую по порядку букву от В в алфавите В-Г-Д; получается первая буква шифртекста - Д.

Следует отметить, что шифр Гронсфельда вскрывается относительно легко, если учесть, что в числовом ключе каждая цифра имеет только десять значений, а значит есть лишь десять вариантов прочтения каждой буквы шифртекста. С другой стороны, шифр Гронсфельда допускает дальнейшие модификации, улучшающие его стойкость, в частности двойное шифрование разными числовыми ключами.

По существу шифр Гронсфельда представляет собой частный случай системы шифрования Вижинера.

Система шифрования Вижинера

Система Вижинера, впервые опубликованная в 1586 г., является одной из старейших и наиболее известных многоалфавитных систем. Свое название она получила по имени французского дипломата XVI в. Блеза Вижинера, который развивал и совершенствовал криптографические системы. Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. На рис. 4 показана таблица Вижинера для русского алфавита.

Таблица Вижинера используется для зашифрования и расшифровки. Таблица имеет два входа: верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста; крайний левый столбец ключа.

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

29	**Э**	**Ю**	**Я**	**А**	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**	**Ы**	**Ъ**
30	**Ю**	**Я**	**А**	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**	**Ы**	**Ъ**	**Э**
31	**Я**	**А**	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**	**Ы**	**Ъ**	**Э**	**Ю**

Рис. 4. Таблица Вижинера

Последовательность ключей обычно получают из числовых значений букв ключевого слова.

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово (или фразу). Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Номер варианта	Текст	Ключевое слово
1.	СТЕГАНОГРАФИЯ СЛУЖИТ ДЛЯ ПЕРЕДАЧИ СЕКРЕТОВ В ДРУГИХ СООБЩЕНИЯХ	АБОНЕНТ
2.	КАК ПРАВИЛО ОТПРАВИТЕЛЬ ПИШЕТ КАКОЕ-НИБУДЬ НЕПРИМЕТНОЕ СООБЩЕНИЕ	СИСТЕМА
3.	ПРИЕМЫ ВКЛЮЧАЮТ НЕВИДИМЫЕ ЧЕРНИЛА, МАЛОПРИМЕТНЫЕ ПОМЕТКИ У БУКВ	РЕШЕНИЕ
4.	В НАСТОЯЩЕЕ ВРЕМЯ ЛЮДИ НАЧАЛИ ПРЯТАТЬ СЕКРЕТЫ В ГРАФИЧЕСКИХ ИЗОБРАЖЕНИЯХ	ТЕХНИКА
5.	В ПЕРЕСТАНОВОЧНОМ ШИФРЕ МЕНЯЕТСЯ НЕ ОТКРЫТЫЙ ТЕКСТ, А ПОРЯДОК СИМВОЛОВ	ПАРТНЕР
6.	КРИПТОГРАФИЯ РЕШАЕТ ПРОБЛЕМЫ СЕКРЕТНОСТИ, ПРОВЕРКИ ПОДЛИННОСТИ, ЦЕЛОСТНОСТИ	ФИНАНСЫ
7.	ПРОТОКОЛ - ЭТО ПОРЯДОК ДЕЙСТВИЙ, ПРЕДПРИНИМАЕМЫХ ДВУМЯ ИЛИ БОЛЕЕ СТОРОНАМИ	АУКЦИОН
8.	ДЕЙСТВИЕ ДОЛЖНО ВЫПОЛНЯТЬСЯ В СВОЮ ОЧЕРЕДЬ И ПОСЛЕ ОКОНЧАНИЯ ПРЕДЫДУЩЕГО	УСЛОВИЕ
9.	КАЖДЫЙ УЧАСТНИК ПРОТОКОЛА ДОЛЖЕН СОГЛАСИТЬСЯ СЛЕДОВАТЬ ПРОТОКОЛУ	ДЕВУШКА
10.	КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ - ЭТО ПРОТОКОЛ, ИСПОЛЬЗУЮЩИЙ КРИПТОГРАФИЮ	ПРИНЦИП
11.	ПОНЯТИЕ ОДНОНАПРАВЛЕННОЙ ФУНКЦИИ ЯВЛЯЕТСЯ ЦЕНТРАЛЬНЫМ В КРИПТОГРАФИИ	ЭКСПЕРТ
12.	ЗНАЮЩИЙ КОМБИНАЦИЮ ЧЕЛОВЕК МОЖЕТ ОТКРЫТЬ СЕЙФ, ПОЛОЖИТЬ В НЕГО ДОКУМЕНТ	ПОЛИЦИЯ
13.	ВСКРЫТИЕ С ВЫБРАННЫМ ОТКРЫТЫМ ТЕКСТОМ МОЖЕТ БЫТЬ ОСОБЕННО ЭФФЕКТИВНЫМ	БУДУЩЕЕ
14.	ИЗ-ЗА НЕДОСТАТКОВ СИСТЕМЫ СИНХРОНИЗАЦИЯ ЧАСОВ МОЖЕТ БЫТЬ НАРУШЕНА	УГЛЕКОП
15.	ОБЫЧНАЯ КРИПТОГРАФИЯ С ОТКРЫТЫМИ КЛЮЧАМИ ИСПОЛЬЗУЕТ ДВА КЛЮЧА	НАПИТОК
16.	ХАКЕР НЕ ПРЕНЕБРЕГАЕТ ОПЕРАТИВНО-ТЕХНИЧЕСКИМИ И АГЕНТУРНЫМИ МЕТОДАМИ	БОТИНОК
17.	ЕСЛИ ВНЕДРЕНИЕ ЗАКЛАДКИ ПРОХОДИТ УСПЕШНО, ВТОРАЯ АТАКА УЖЕ НЕ ТРЕБУЕТСЯ	ДЕРЗКИЙ
18.	ХАКЕР ЗАРАНЕЕ ПРОДУМЫВАЕТ ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ НЕУДАЧИ	СИМПТОМ
19.	ПРОГРАММНАЯ ЗАКЛАДКА, ВНЕДРЕННАЯ В СИСТЕМУ, ЗАМЕТНА ТОЛЬКО ХАКЕРУ	ЧЕМОДАН
20.	С ТОЧКИ ЗРЕНИЯ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМА РАБОТАЕТ КАК ОБЫЧНО	ЭСКУЛАП

Контрольные вопросы.

1. Приведите примеры шифров перестановки.
2. Сформулируйте общие принципы для методов шифрования подстановкой.

3. В чем заключаются многоалфавитные подстановки?

4. Приведите пример шифра одноалфавитной замены.

5. Опишите алгоритм любого метода шифрования перестановкой. Приведите пример шифрования некоторого сообщения этим методом. Каков алгоритм расшифрования в этом методе?

6. К какой группе методов шифрования с закрытым ключом относится метод с использованием таблицы Вижинера? Каковы алгоритмы шифрования и расшифрования в этом методе? Приведите пример шифрования некоторого сообщения этим методом.

7. Каким образом можно зашифровать и расшифровать сообщение методом табличной перестановки, если размер шифруемого сообщения не кратен размеру блока?

Лабораторная работа 4. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации.

Цель. Научиться разрабатывать программы разграничения полномочий пользователей на основе парольной аутентификации

Задание

1. Программа должна обеспечивать работу в двух режимах: администратора (пользователя с фиксированным именем ADMIN) и обычного пользователя.

2. В режиме администратора программа должна поддерживать следующие функции (при правильном вводе пароля):

- смена пароля администратора (при правильном вводе старого пароля);
- просмотр списка имен зарегистрированных пользователей и установленных для них параметров (блокировка учетной записи, включение ограничений на выбираемые пароли) – всего списка целиком в одном окне или по одному элементу списка с возможностью перемещения к его началу или концу;
- добавление уникального имени нового пользователя к списку с пустым паролем (строкой нулевой длины);
- блокирование возможности работы пользователя с заданным именем;
- включение или отключение ограничений на выбираемые пользователем пароли (в соответствии с индивидуальным заданием, определяемым номером варианта);
- завершение работы с программой.

3. В режиме обычного пользователя программа должна поддерживать только функции смены пароля пользователя (при правильном вводе старого пароля) и завершения работы, а все остальные функции должны быть заблокированы.

4. После своего запуска программа должна запрашивать у пользователя в специальном окне входа ввод его имени и пароля. При вводе пароля его символы всегда должны на экране заменяться символом ‘*’.

5. При отсутствии введенного в окне входа имени пользователя в списке зарегистрированных администратором пользователей программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода имени или завершения работы с программой.

6. При неправильном вводе пароля программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода. При трехкратном вводе неверного пароля работа программы должна завершаться.

7. При первоначальном вводе пароля (обязательном при первом входе администратора или пользователя с зарегистрированным ранее администратором именем) и при дальнейшей замене пароля программа должна просить пользователя подтвердить введенный пароль путем его повторного ввода.

8. Если выбранный пользователем пароль не соответствует требуемым ограничениям (при установке соответствующего параметра учетной записи пользователя), то программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность ввода другого

пароля, завершения работы с программой (при первом входе данного пользователя) или отказа от смены пароля.

9. Информация о зарегистрированных пользователях, их паролях, отсутствии блокировки их работы с программой, а также включении или отключении ограничений на выбираемые пароли должна сохраняться в специальном файле. При первом запуске программы этот файл должен создаваться автоматически и содержать информацию только об администраторе, имеющем пустой пароль.

10. Интерфейс с программой должен быть организован на основе меню, обязательной частью которого должно являться подменю «Справка» с командой «О программе». При выборе этой команды должна выдаваться информация об авторе программы и выданном индивидуальном задании. Интерфейс пользователя программы может также включать панель управления с дублирующими команды меню графическими кнопками и строку состояния.

11. Для реализации указанных в пунктах 2-3 функций в программе должны использоваться специальные диалоговые формы, позволяющие пользователю (администратору) вводить необходимую информацию.

Индивидуальные варианты заданий (ограничения на выбираемые пароли)

1. Длина не меньше минимальной длины, устанавливаемой администратором и сохраняемой в учетной записи пользователя.
2. Наличие строчных и прописных букв.
3. Наличие букв и цифр.
4. Наличие букв и знаков препинания.
5. Наличие цифр и знаков препинания.
6. Наличие букв и знаков арифметических операций.
7. Наличие цифр и знаков арифметических операций.
8. Наличие латинских букв и символов кириллицы.
9. Наличие букв, цифр и знаков препинания.
10. Наличие латинских букв, символов кириллицы и цифр.
11. Наличие латинских букв, символов кириллицы и знаков препинания.
12. Наличие строчных и прописных букв, а также цифр.
13. Наличие строчных и прописных букв, а также знаков препинания.
14. Наличие строчных и прописных букв, а также знаков арифметических операций.
15. Наличие латинских букв, символов кириллицы и знаков арифметических операций.
16. Наличие букв, цифр и знаков арифметических операций.
17. Наличие букв, знаков препинания и знаков арифметических операций.
18. Наличие цифр, знаков препинания и знаков арифметических операций.
19. Отсутствие повторяющихся символов.
20. Чередование букв, цифр и снова букв.
21. Чередование букв, знаков препинания и снова букв.

Контрольные вопросы

1. Что такое идентификация?
2. Что такое аутентификация?
3. Правила выбора и использования пароля.
4. Объекты идентификации и установления подлинности в информационной системе.
5. Особенности разделения привилегий и разграничения доступа?
6. Меры предосторожности, которые необходимо соблюдать при использовании пароля?
7. Аутентификация пользователей на основе паролей.

Лабораторная работа 5. Использование функций криптографического интерфейса *Windows* для защиты информации.

Цель. Изучить функции криптографического интерфейса Windows для защиты информации

Задание

1. В программу, разработанную при выполнении лабораторной работы 3, добавить средства защиты от несанкционированного доступа к файлу с учетными данными зарегистрированных пользователей.

2. Файл с учетными данными должен быть зашифрован при помощи функций криптографического интерфейса операционной системы Windows (CryptoAPI) с использованием сеансового ключа, генерируемого на основе вводимой администратором (пользователем) парольной фразы.

3. При запуске программы файл с учетными данными должен расшифровываться во временный файл (или в файл в оперативной памяти), который после завершения работы программы должен быть снова зашифрован для отражения возможных изменений в учетных записях пользователей. «Старое» содержимое файла учетных записей при этом стирается.

4. После ввода парольной фразы при запуске программы, генерации ключа расшифрования и расшифрования файла с учетными данными зарегистрированных пользователей правильность введенной парольной фразы определяется по наличию в расшифрованном файле учетной записи администратора программы.

5. При вводе неправильной парольной фразы или отказе от ее ввода работа программы должна завершаться с выдачей соответствующего сообщения.

6. Временный файл на диске с расшифрованными учетными данными после завершения работы программы удаляется.

7. Варианты использования алгоритмов шифрования и хеширования выбираются в соответствии с выданным преподавателем заданием.

Индивидуальные варианты заданий

№	Тип симметричного шифрования	Используемый режим шифрования	Добавление к ключу случайного значения	Используемый алгоритм хеширования
1	Блочный	Электронная кодовая книга	Да	MD2
2	Потоковый	-	Да	MD2
3	Блочный	Сцепление блоков шифра	Да	MD2
4	Потоковый	-	Да	MD5
5	Блочный	Обратная связь по шифротексту	Да	MD2
6	Потоковый	-	Да	SHA
7	Блочный	Электронная кодовая книга	Да	MD4
8	Потоковый	-	Нет	MD2
9	Блочный	Сцепление блоков шифра	Да	MD4
10	Потоковый	-	Нет	MD5
11	Блочный	Обратная связь по шифротексту	Да	MD4
12	Потоковый	-	Нет	SHA
13	Блочный	Электронная кодовая книга	Да	MD5
14	Блочный	Сцепление блоков шифра	Да	MD5
15	Блочный	Обратная связь по шифротексту	Да	MD5
16	Блочный	Электронная кодовая книга	Да	SHA
17	Блочный	Сцепление блоков шифра	Да	SHA
18	Блочный	Обратная связь по шифротексту	Да	SHA
19	Блочный	Электронная кодовая книга	Нет	MD2
20	Блочный	Сцепление блоков шифра	Нет	MD2
21	Блочный	Обратная связь по шифротексту	Нет	MD2
22	Блочный	Электронная кодовая книга	Нет	MD4
23	Блочный	Сцепление блоков шифра	Нет	MD4

Контрольные вопросы

1. На чем основаны криптографические методы и средства защиты информации?
2. Как осуществляется несимметричное шифрование данных?
3. Применение криптографического интерфейса Windows для защиты информации.
4. Охарактеризуйте особенности криптографической защиты информации.
5. Приведите специализированные программные средства защиты от несанкционированного доступа в защищенных операционных системах.

Лабораторная работа 6. Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей.

Цель: реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

Задание.

1. В таблице найти для указанного варианта значения характеристик *P, V, T*.

2. Вычислить по формуле (1) нижнюю границу *S** для заданных *P, V, T*.

3. Выбрать некоторый алфавит с мощностью *A* и получить минимальную длину пароля *L*, при котором выполняется условие (2).

4. Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины *L*, при этом должен использоваться алфавит из *A* символов.

5. Оформить отчет по лабораторной работе.

Коды символов:

1. Коды английских символов : «A» = 65, …, «Z» = 90, «a» = 97,…, «z» = 122.

2. Коды цифр : «0» = 48, «9» = 57.

3. «!» = 33, «“» = 34, «#» = 35, «$» = 36, «%» = 37, «&» = 38, «‘» = 39.

4. Коды русских символов : «А» – 128, … «Я» – 159, «а» – 160,…, «п» – 175, «р» – 224,…, «я» – 239.

Теоретические сведения

Подсистемы идентификации и аутентификации пользователя играют важную роль в системах защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации являются одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя, как правило, передний край обороны СЗИ. В связи с этим модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель последнего в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя наиболее просты и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю:

1) минимальная длина пароля должна быть не менее 6 символов;

2) пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.);

3) в качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

К подсистеме парольной аутентификации:

1) администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, пароль следует сменить;

2) в подсистеме парольной аутентификации необходимо установить ограничение числа попыток ввода пароля (как правило, не более трёх);

3) в подсистеме парольной аутентификации требуется установить временную задержку в случае ввода неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля: если пароль состоит только из малых английских букв, то $A = 26$), L – длина пароля, $S = A^L$ – число всевозможных паролей длины L, которые можно составить из символов алфавита A, V – скорость перебора паролей злоумышленником, T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течение срока его действия V определяется по следующей формуле:

$P = (V \cdot T) / S = (V \cdot T) / A^L$.

Эту формулу можно использовать в обратную сторону для решения следующей задачи.

Задача. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Данная задача имеет неоднозначное решение. При исходных данных V, T, P однозначно можно определить лишь нижнюю границу S^* числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле

$$S^* = [V \cdot P / T], \quad (1)$$

где [] – целая часть числа, взятая с округлением вверх.

После определения нижней границы S^* необходимо выбрать такие A и L для формирования $S = A^L$, чтобы выполнялось следующее неравенство:

$$S^* \le S = A^L. \quad (2)$$

При выборе S, удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P.

Следует отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

Пример. Исходные данные: $P = 10^{-6}$, $T = 7$ дней = 1 неделя, $V = 10$ (паролей / минуту) = $10 \cdot 60 \cdot 24 \cdot 7 = 100800$ паролей в неделю. Тогда, $S^* = [(10800 \cdot 1) / 10^{-6}] = = 108 \cdot 10^8$.

Условию $S^* \le A^L$ удовлетворяют, например, такие комбинации A и L, как $A = 26$, $L = 8$ (пароль состоит из восьми малых символов английского алфавита), $A = 36$, $L = 6$ (пароль состоит из шести символов, среди которых могут быть малые латинские буквы и произвольные цифры).

Таблица – Варианты заданий

Вариант	P	V	T
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
13	10^{-4}	10 паролей/день	5 дней
14	10^{-5}	20 паролей/мин	6 дней
15	10^{-6}	15 паролей/мин	12 дней

16	10^{-7}	3 паролей/мин	1 месяц
17	10^{-4}	10 паролей/мин	3 недели
18	10^{-5}	11 паролей/мин	20 дней
19	10^{-6}	100 паролей/день	15 дней
20	10^{-7}	10 паролей/день	1 неделя

Контрольные вопросы

1. Чем определяется стойкость подсистемы идентификации и аутентификации?
2. Перечислить минимальные требования к выбору пароля.
3. Перечислить минимальные требования к подсистеме парольной аутентификации.
4. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?
5. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ СТУДЕНТОВ

Самостоятельная работа развивает мотивационную составляющую образовательной деятельности студентов, акцентируясь на самообразовании и самовоспитании, осуществляемых в интересах повышения профессиональной компетенции. Она развивает систему общеучебных умений, способствующих ее рациональной организации:

- планировать собственную образовательную деятельность,
- четко ставить систему задач,
- вычленять среди них главные направления работы,
- избирать способы наиболее быстрого и экономного решения поставленных задач,
- осуществлять оперативный контроль за выполнением задания,
- оперативно вносить коррективы в самостоятельную работу, анализировать промежуточные и общие итоги работы,
- сравнивать полученные результаты с намеченными в начале работы целями, выявлять причины отклонений и определять пути их коррекции в дальнейшей работе.

Самостоятельная работа включает два вида – аудиторную и внеаудиторную.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Основными видами аудиторной самостоятельной работы являются:

−выполнение лабораторных и практических работ по инструкциям; работа с литературой и другими источниками информации, в том числе электронными;

−само- и взаимопроверка выполненных заданий;

−решение проблемных и ситуационных задач.

Выполнение лабораторных осуществляется на лабораторных занятиях в соответствии с графиком учебного процесса.

Работа с литературой, другими источниками информации, в т.ч. электронными может реализовываться на семинарских и практических занятиях. Данные источники информации могут быть представлены на бумажном и/или электронном носителях, в том числе, в сети Internet. Преподаватель формулирует цель работы с данным источником информации, определяет время на проработку документа и форму отчетности.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя, но без его непосредственного участия.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня подготовленности обучающихся.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

– для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы); составление плана текста; графическое изображение структуры текста; конспектирование текста; выписки из текста; работа со словарями и справочниками; учебно-исследовательская работа; использование аудио- и видеозаписей, компьютерной техники и Интернет-ресурсов и др.;
– для закрепления и систематизации знаний: работа с конспектом лекции (обработка текста); повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио- и видеозаписей); составление плана и тезисов ответа; составление таблиц, ребусов, кроссвордов, глоссария для систематизации учебного материала; изучение словарей, справочников; ответы на контрольные вопросы; аналитическая обработка текста (аннотирование, рецензирование, реферирование, контент-анализ и др.); подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов; составление библиографии, заданий в тестовой форме и др.;
– для формирования умений: решение задач и упражнений по образцу; решение вариативных задач и упражнений; составление схем; решение ситуационных производственных (профессиональных) задач; подготовка к деловым и ролевым играм; проектирование и моделирование разных видов и компонентов профессиональной деятельности; подготовка презентаций, творческих проектов; подготовка курсовых и выпускных работ; опытно-экспериментальная работа; проектирование и моделирование разных видов и компонентов профессиональной деятельности и др.

Преподаватель осуществляет управление самостоятельной работой, регулирует ее объем на одно учебное занятие и осуществляет контроль выполнения всеми обучающимися группы. Для удобства преподаватель может вести ведомость учета выполнения самостоятельной работы, что позволяет отслеживать выполнение минимума заданий, необходимых для допуска к итоговой аттестации по дисциплине.

В процессе самостоятельной работы студент приобретает навыки самоорганизации, самоконтроля, самоуправления и становится активным самостоятельным субъектом учебной деятельности.

Обучающийся самостоятельно определяет режим своей внеаудиторной работы и меру труда, затрачиваемого на овладение знаниями и умениями по каждой дисциплине, выполняет внеаудиторную работу по индивидуальному плану, в зависимости от собственной подготовки, бюджета времени и других условий.

Ежедневно обучающийся должен уделять выполнению внеаудиторной самостоятельной работы в среднем не менее 3 часов.

При выполнении внеаудиторной самостоятельной работы обучающийся имеет право обращаться к преподавателю за консультацией с целью уточнения задания, формы контроля выполненного задания.

Контроль результатов внеаудиторной самостоятельной работы студентов может проводиться в письменной, устной или смешанной форме с представлением продукта деятельности обучающегося. В качестве форм и методов контроля внеаудиторной самостоятельной работы могут быть использованы зачеты, тестирование, самоотчеты, контрольные работы, защита творческих работ и др.

Подготовка к экзамену: один из самых ответственных видов самостоятельной работы, и в то же время возможность сэкономить большое количество времени в период сессии, если эту подготовку начинать заблаговременно. Одно из главных правил – представлять себе общую логику предмета, что достигается проработкой планов лекций, составлением опорных конспектов, схем таблиц. Фактически основной вид полготовки к экзамену – «свертывание» большого объема информации в компактный вид, а также тренировка в ее «развертывании» (примеры к теории, выведение одних закономерностей из других и т.д.). Владение этими технологиями обеспечивает, пожалуй, более половины успеха. Тем более что преподаватель обычно замечает в течение семестра целенаправленную подготовку такого студента и может поощрить его тем или иным способом. Надо также правильно распределить силы, не только готовясь к самому экзамену,

но. Наконец, необходимо выяснить условия проведении, самого экзаменационного испытания, использовав для этой цели прежде всего консультацию (хотя преподаватель обычно касается этой темы заранее): количество и характер вопросов, форма проведения (устно или письменно), возможность использовать при подготовке различные материалы и по собия (таблицы, схемы, тетради для практических занятий и т.д.).

ЛИТЕРАТУРА

1. Аверченков, В. И. Организационная защита информации : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. – Москва : Изд-во «ФЛИНТА», 2011. – 184 с.

2. Основы организованного обеспечения информационной безопасности объектов информатизации / С. Н. Сёмкин, Э. В. Беляков, С. В. Гребенев, В. И. Козачок. – Москва : Изд-во «Гелиос АРВ», 2005.

3. Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – Москва : Горячая линия – Телеком, 2006. – 544 с.

4. Организационно-правовое обеспечение информационной безопасности : учебное пособие / А. А. Стрельцов, В. С. Горбатов, Т. А. Полякова [и др.]; под ред. А. А. Стрельцова. – Москва : Издательский центр «Академия», 2008. – 256 с.

5. Мельников, П. В. Информационная безопасность и защита информации / П. В. Мельников, С. А. Клейменов, А. М. Петраков. – 6-е изд. – Издательский центр «Академия», 2012.

6. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости./ М., 2007, 254 с.

7. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ В.Ф. Шаньгин— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 544 c.— Режим доступа: http://www.iprbookshop.ru/63592.html.— ЭБС «IPRbooks»

8. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Д.А. Скрипник— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 c.— Режим доступа: http://www.iprbookshop.ru/52161.html. — ЭБС «IPRbooks»

СОДЕРЖАНИЕ