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

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

сборник учебно-методических материалов

для направления подготовки 10.03.01 Информационная безопасность

Благовещенск

2019

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

Составитель: Самохвалова С.Г.

Основы информационной безопасности: сборник учебно-методических материалов для направления подготовки 10.03.01 Информационная безопасность – Благовещенск: Амурский гос. ун-т, 2019

КРАТКОЕ ИЗЛОЖЕНИЕ ЛЕКЦИОННОГО МАТЕРИАЛА

Свойства информации как объекта защиты

Что такое «информация»? Ответить достаточно сложно.

На обще лексическом, бытовом уровне понятие «информация» обычно толкуется как «сообщение, осведомляющее о положении дел, о состоянии чего-нибудь». Заметим, что и в нормативных правовых актах чаще всего данное понятие употребляется именно в этом смысле.

Информация первична и содержательна - это категория, поэтому в категориальный аппарат науки она вводится описанием, через близкие категории: материя, система, структура, отражение. С информацией связаны понятия – знание, данные, сигналы, сообщения, смысл, семантика. Не следует путать категорию информация с понятием знание. Знание определяется через категорию информация.

В материальном мире человека информация материализуется через свой носитель и благодаря ему существует. Сущность материального мира предстаёт перед исследователем в единстве формы и содержания. Передаётся информация через носитель. Материальный носитель придаёт информации форму. В процессе формообразования производится смена носителя информации.

В XX веке слово «информация» стало термином во множестве научных областей, получив особые для них определения и толкования.

Научное знание начинается с определений и классификации. Не станем пренебрегать этой традицией. Прежде всего необходимо разобраться в сущности того, что и от чего необходимо защищать. Но отвечая на вопрос о том, что такое информация, можно легко зайти в тупик. Затратив сравнительно немного времени, мы обнаружим массу определений слова «информация».

Некоторые из них приводятся ниже в порядке возрастания длины их формулировки (к сожалению, установить авторов ряда определений не удалось).

1. Информация – это знания (вариант – новые знания).
2. Информация – это вероятность выбора (И. М. Яглом).
3. Информация – это отраженное разнообразие (А. Д. Урсул)
4. Информация – это мера сложности объекта (А. Н. Колмогоров).
5. Информация – это информация, а не вещество и не энергия (Н. Винер).
6. Информация – это функция целевой интерпретации полученного сообщения.
7. Информация определяется только вероятностными свойствами сообщений (К. Шеннон).
8. Информация – это отражение объективной реальности в сознании человека (В. И. Ленин).
9. Информация – это мера зависимости случайных переменных или мера организации системы.
10. Информация – это свойство материи, отличное от ее вещественных и энергетических свойств.
11. Информация – это сведения об окружающем мире и протекающих в нем процессах (С. И. Ожегов).
12. Информация – это сведения, которые уменьшают или снимают неразличимость вещей или явлений.
13. Информация – это сведения, которые снимают неопределенность, существующую до их получения.
14. Информация об объекте есть изменение параметра наблюдателя, вызванное взаимодействием наблюдателя с объектом (В. И. Шаповалов).
15. Информация – это обозначение содержания, черпаемого нами из внешнего мира в процессе приспособления к нему и приведения в соответствие с ним нашего мышления (Н. Винер)
16. Информация – это сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.06 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).
17. Информация – это универсальная субстанция, пронизывающая все сферы человеческой деятельности, служащая проводником знаний и мнений, инструментом общения, взаимопонимания и сотрудничества, утверждения стереотипов мышления и поведения (ЮНЕСКО).

18. Информация – это сведения о фактах, событиях, процессах и явлениях, о состоянии (свойствах, характеристиках) в некоторой предметной области, воспринимаемые человеком или специальным устройством и используемые (необходимые) для оптимизации принимаемых решений в процессе управления данными объектами (Д. И. Правиков).

Эти определения приведены не с целью их заучивания и не для того, чтобы на их основе пытаться сформулировать законченное и безусловно верное определение информации. Следует отметить, что в данном перечне нет принципиально неверных определений, все они так или иначе справедливы. И в то же время ни одно из них не может претендовать на полноту. Ответ очевиден: человечество (точнее, его передовые умы) до сих пор не определилось в отношении того, что такое информация. Н. Н. Моисеев объяснил это так: «Достаточно универсального определения быть просто не может, ибо оно неотделимо от свойств субъекта, который нуждается не в информации вообще, а во вполне определенной информации» .

Но для решения задачи о способах и средствах надежного хранения информации нам и не потребуется ее полного и строгого определения, подобно тому как надежная защита драгоценностей от хищения вовсе не требует знания их физических и химических свойств. Для принятия решения о выборе способа и места надежного хранения ценности достаточно знать ее рыночную стоимость и условия, в которых она не потеряет своих потребительских свойств.

Чтобы зафиксировать термин для дальнейшего обращения с ним воспользуемся Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Итак, «**информация** - сведения (сообщения, данные) независимо от формы их представления».

В общем, это согласуется с трактовкой информации в справочной философской литературе последнего времени как «одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.».

Особо можно выделить понятие

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Согласно ФЗ № 149-ФЗ, 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**).

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. «Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

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

Кроме того, по закону, информация в зависимости **от порядка предоставления или распространения** подразделяется на информацию:

1) свободно распространяемую;
2) предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3) подлежащую предоставлению или распространению в соответствии с федеральными законами;
4) ограниченную или запрещенную для распространения в Российской Федерации.

Закон РФ «О средствах массовой информации», принятый в 1991 году, определяет понятие «**массовая информация»,** как «предназначенные для неограниченного круга лиц печатные, аудиовизуальные и иные сообщения и материалы».

Чтобы определить, что такое «информационная безопасность», рассмотрим сначала само понятие «**безопасности**». Здесь тоже имеет место различие мнений и определений.

Вл. Даль определял, что «**безопасность** – есть отсутствие опасности, сохранность, надежность».

В толковом словаре русского языка Ожегова С.И. сказано, что « **безопасность** – состояние, в котором не угрожает опасность, есть защита от опасности».

Закон «О безопасности» 1992 года гласит, что «**безопасность** – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних **угроз**». Появилось новое понятие «угрозы», близкое к понятию «опасности», упоминавшихся у Даля и Ожегова.

Понятие государственной тайны.

Исполнение Закона РФ "О государственной тайне" организует правительство РФ. Оно же представляет на утверждение президенту РФ состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней; представляет на утверждение Президенту РФ Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне.

В свою очередь президент РФ утверждает состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней; перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также перечень сведений, отнесенных к государственной тайне; заключает международные договоры РФ о совместном использовании и защите сведений, составляющих государственную тайну; определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента РФ; в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

В ст.2 Закона определены некоторые термины, составляющие сущность закона.

Носители сведений, составляющих государственную тайну, – это материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Система защиты государственной тайны определена как совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях.

Допуск к государственной тайне понимается в законе как процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений.

Гриф секретности – это реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

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.

Президент Российской Федерации: утверждает по представлению Правительства Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней; утверждает по представлению Правительства Российской Федерации Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне; заключает международные договоры Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну; определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента Российской Федерации; в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

Перечень сведений, составляющих государственную тайну

Согласно II разделу Закона государственную тайну составляют:

1) сведения в военной области:

- о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;
- о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;
- о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;
- о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;
- о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;
- о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состояния их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

- о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;
- об использовании инфрастуктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;
- о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;
- об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;
- о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;
- об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых РФ (по списку, определяемому Правительством РФ);

3) сведения в области внешней политики и экономики:

- о внешнеполитической, внешнеэкономической деятельности РФ, преждевременное распространение которых может нанести ущерб безопасности государства;
- о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной

деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

- о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
- о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;
- об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
- о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;
- о методах и средствах защиты секретной информации;
- об организации и о фактическом состоянии защиты государственной тайны;
- о защите Государственной границы РФ, исключительной экономической зоны и континентального шельфа РФ;
- о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в РФ;
- о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

Актуальность проблемы обеспечения безопасности информации

Понятие «информация» сегодня употребляется весьма широко и разносторонне. Трудно найти такую область знаний, где бы оно не использовалось. Огромные информационные потоки буквально захлестывают людей.

На общеупотребительном уровне информация выступает как совокупность данных об экономической ситуации, доведенных до сведения агентов институтами статистики, органами прогнозирования или же органами содействия принятию решения.

В экономическом аспекте информация - специфический товар, обусловливающий неравенство (асимметрию) на рынке и по своим свойствам подчиняющийся экономике информационного производства.

В законе РФ об ***«Информации, информационных технологиях и защите информации»,*** определено: «**информация** - сведения (сообщения, данные) независимо от формы их представления».

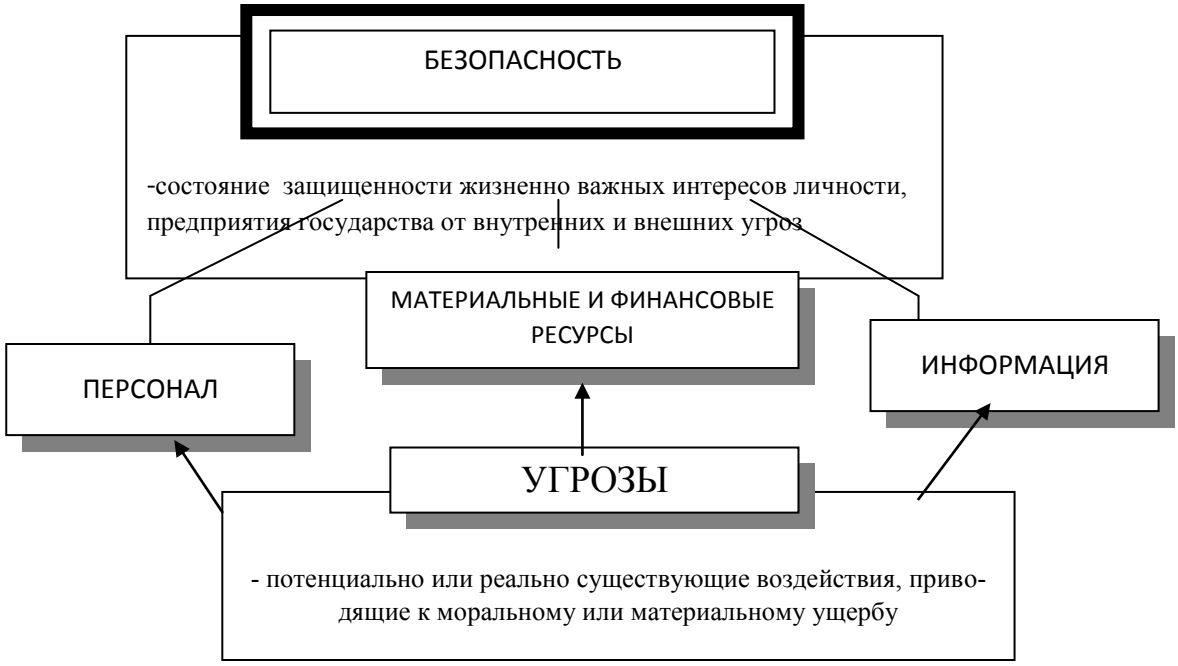
Как и всякий продукт, информация имеет потребителей, нуждающихся в ней, и потому обладает определенными потребительскими качествами, а также имеет и своих обладателей или производителей.

С точки зрения потребителя, качество используемой информации позволяет получать дополнительный экономический или моральный эффект.

С точки зрения обладателя — сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту конфиденциальной информации.

Понимая под безопасностью состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз, можно выделить и компоненты безопасности — такие, как персонал, материальные и финансовые средства и информацию.

Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляю весьма развитый арсенал программных и аппаратных средств защиты информации, производимых на промышленной основе; значительное число фирм, специализирующихся на решении вопросов защиты информации; достаточно четко очерченная система взглядов на эту проблему; наличие значительного практического опыта и другое.



Как свидетельствует отечественная и зарубежная печать, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту.

Последнее время сообщения об атаках на информацию, о хакерах и компьютерных взломах наполнили все средства массовой информации. Что же такое "атака на информацию"? Дать определение этому действию на самом деле очень сложно, поскольку информация, особенно в электронном виде, представлена сотнями различных видов. Информацией можно считать и отдельный файл, и базу данных, и одну запись в ней, и целиком программный комплекс. И все эти объекты могут подвергнуться и подвергаются атакам со стороны некоторой социальной группы лиц.

При хранении, поддержании и предоставлении доступа к любому информационному объекту его владелец, либо уполномоченное им лицо, накладывает набор правил по работе с ней. Умышленное их нарушение классифицируется как атака на информацию.

С массовым внедрением компьютеров во все сферы деятельности человека объем информации, хранимой в электронном виде вырос в тысячи раз. И теперь скопировать за полминуты и унести USB-устройство с файлом, содержащим план выпуска продукции, намного проще, чем копировать или переписывать кипу бумаг. А с появлением компьютерных сетей даже отсутствие физического доступа к компьютеру перестало быть гарантией сохранности информации.

Для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов. Причем в этом должны активно участвовать профессиональные специалисты, администрация, сотрудники и пользователи, что и определяет повышенную значимость организационной стороны вопроса.

Опыт показывает, что:

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

безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм — систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий;

никакая СЗИ не может обеспечить требуемого уровня безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех установленных правил, направленных на ее защиту

С учетом накопленного опыта можно определить систему защиты информации как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

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

непрерывной. Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;

плановой. Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);

целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;

конкретной. Защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;

активной. Защищать информацию необходимо с достаточной степенью настойчивости;

надежной. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;

универсальной. Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;

комплексной. Для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства. Комплексный характер защиты проистекает из того, что защита — это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов.

Зарубежный и отечественный опыт показывает, что для обеспечения выполнения столь многогранных требований безопасности система защиты информации должна удовлетворять определенным условиям:

• охватывать весь технологический комплекс информационной деятельности;

• быть разнообразной по используемым средствам, многоуровневой с иерархической последовательностью доступа;

• быть открытой для изменения и дополнения мер обеспечения безопасности информации;

• быть нестандартной, разнообразной. При выборе средств защиты нельзя рассчитывать на неосведомленность злоумышленников относительно ее возможностей;

• быть простой для технического обслуживания и удобной для эксплуатации пользователями;

• быть надежной. Любые поломки технических средств являются причиной появления неконтролируемых каналов утечки информации;

• быть комплексной, обладать целостностью, означающей, что ни одна ее часть не может быть изъята без ущерба для всей системы.

К системе безопасности информации предъявляются также определенные 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, как любая система, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого СЗИ может иметь:

• правовое обеспечение. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия;

• 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 деятельность и другими;

• аппаратное обеспечение. Предполагается широкое использование технических средств как для защиты информации, так и для обеспечения деятельности собственно СЗИ;

• 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;

• 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;

• математическое обеспечение. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;

• лингвистическое обеспечение. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

• 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.

Основные составляющие информационной безопасности

Информационная безопасность - многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Поясним понятия доступности, целостности и конфиденциальности.

Доступность — это возможность за приемлемое время получить требуемую информационную услугу.

Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность - это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления — производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия — и материальные, и моральные — может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит "руководством к действию". Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса - все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница WeЬ-сервера какой-либо правительственной организации.

Конфиденциальность - самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Конфиденциальные моменты есть также у многих организаций и отдельных пользователей (например, пароли).

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.

Концептуальная модель информационной безопасности.

Понимая информационную безопасность как «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций», правомерно определить угрозы безопасности информации, источники этих угроз, способы их реализации и цели, а также иные условия и действия, нарушающие безопасность. При этом, естественно, следует рассматривать и меры защиты информации от неправомерных действий, приводящих к нанесению ущерба.

Практика показала, что для анализа такого значительного набора источников, объектов и действий целесообразно использовать методы моделирования, при которых формируется как бы «заместитель» реальных ситуаций. При этом следует учитывать, что модель не копирует оригинал, она проще. Модель должна быть достаточно общей, чтобы описывать реальные действия с учетом их сложности.

Можно предложить компоненты модели информационной безопасности на первом уровне декомпозиции. По нашему мнению, такими компонентами концептуальной модели безопасности информации могут быть следующие: объекты угроз; угрозы; источники угроз; цели угроз со стороны злоумышленников; источники информации; способы неправомерного овладения конфиденциальной информацией (способы доступа); направления защиты информации; способы защиты информации; средства защиты информации.

Объектами угроз информационной безопасности выступают *сведения о составе, состоянии и деятельности объекта защиты* (персонала, материальных и финансовых ценностей, информационных ресурсов). *Угрозы информации* выражаются *в нарушении ее доступности, целостности и конфиденциальности*. *Источниками угроз* выступают *конкуренты, преступники, коррупционеры, административно-управленческие органы*.

Источники угроз преследуют при этом следующие цели: *ознакомление* с охраняемыми сведениями, их *модификация* в корыстных целях и *уничтожение* для нанесения прямого материального ущерба.

Неправомерное овладение конфиденциальной информацией возможно за счет ее *разглашения* источниками сведений, за счет *утечки* информации через технические средства и за счет *несанкционированного доступа* к охраняемым сведениям.

Источниками конфиденциальной информации являются *люди, документы, публикации, технические носители информации, технические средства* обеспечения производственной и трудовой деятельности, *продукция* и *отходы* производства.

Основными *направлениями защиты* информации являются *правовая, организационная и инженерно-техническая защиты*информации как выразители комплексного подхода к обеспечению информационной безопасности. *Средствами защиты* информации являются *физические сред-*

ства, аппаратные средства, программные средства и криптографические методы. Последние могут быть реализованы как аппаратно, программно, так и смешанно-программно-аппаратными средствами. В качестве *способов защиты* выступают всевозможные меры, пути, способы и действия, обеспечивающие *упреждение* противоправных действий, их *предотвращение*, *пресечение* и *противодействие* несанкционированному доступу.

В обобщенном виде рассмотренные компоненты в виде концептуальной модели безопасности информации приведены на следующей схеме (рис. 1).

Рис.1. Концептуальная модель безопасности информации

В конечном итоге противоправные действия с информацией приводят к нарушению ее конфиденциальности, целостности и доступности, что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации.

Угрозы информационной безопасности. Виды противников и каналы утечки информации.

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

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).

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.

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

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 (чаше 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 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 денежное 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 каналам радиосвязи
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 ПО. Компьютерные вирусы и средства защиты от них

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 разрушительным 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 дру-

гих 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 программного 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.

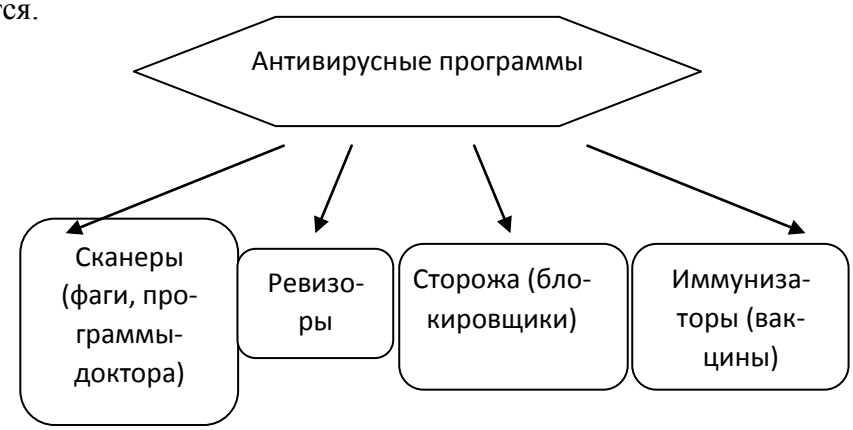
Различают следующие виды антивирусных программ:

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 прове-

ряемого 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.

Необходимость в проактивной защите назрела с тех пор, как скорость распространения вредоносных программ стала превышать скорость обновления антивирусной защиты, способной обезвредить эти угрозы. Реактивные технологии, на которых построена антивирусная защита, требуют как минимум одного фактического заражения новой угрозой, времени на анализ вредоносного кода, на добавление его в базы сигнатур угроз и на обновление этой базы на компьютерах пользователей. За это время новая угроза может нанести огромный ущерб.

Управление рисками

Управление рисками, актуально только для тех организаций, *информационные системы* которых и/или обрабатываемые данные можно считать нестандартными. Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области ИБ). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими параметрами.

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный *ущерб* неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая (пере) ***оценка рисков*** необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения уровень риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимые места), а также величины возможного ущерба.

Таким образом, суть мероприятий *по* управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, *управление рисками* включает в себя два вида деятельности, которые чередуются циклически:

- (пере)оценка (измерение) рисков;
- выбор эффективных и экономичных защитных средств (*нейтрализация рисков*).

По отношению к выявленным рискам возможны следующие действия:

- ***ликвидация риска*** (например, за счет устранения причины);
- ***уменьшение риска*** (например, за счет использования дополнительных защитных средств);
- ***принятие риска*** (и выработка плана действия в соответствующих условиях);
- ***переадресация риска*** (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на следующие этапы:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор ***методологии оценки рисков***.
3. ***Идентификация активов***.
4. ***Анализ угроз*** и их последствий, ***выявление уязвимых мест*** в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка ***остаточного риска***.

Этапы 6 и 7 относятся к выбору защитных средств (нейтрализации рисков), остальные - к оценке рисков.

Уже *перечисление* этапов показывает, что *управление рисками* - процесс циклический. *По* существу, последний этап - это оператор конца *цикла*, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую *деятельность*.

Управление рисками, как и любую другую *деятельность* в области информационной безопасности, необходимо интегрировать в *жизненный цикл ИС*. Тогда эффект оказывается наибольшим, а *затраты* - минимальными. Ранее мы определили пять этапов жизненного *цикла*. Кратко опишем, что может дать управление рисками на каждом из них.

На этапе ***инициации*** известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности.

На этапе ***закупки (разработки)*** знание рисков поможет выбрать соответствующие архитектурные решения, которые играют ключевую роль в обеспечении безопасности.

На этапе ***установки*** выявленные риски следует учитывать при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный *цикл управления* рисками должен предшествовать внедрению системы в эксплуатацию.

На этапе ***эксплуатации*** управление рисками должно сопровождать все существенные изменения в системе.

При ***выведении системы из эксплуатации*** управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

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 потребитель-

ские 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 обслуживанием 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

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:

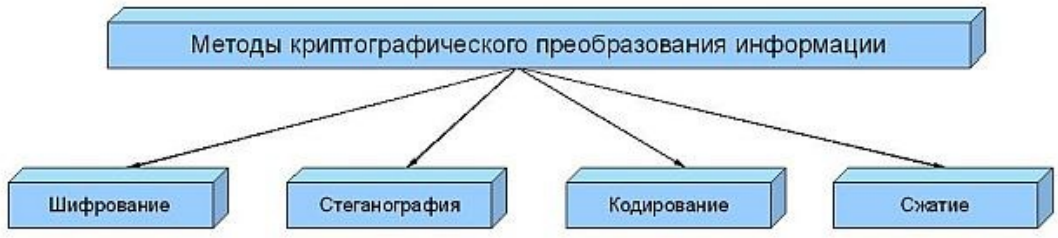


Рис. 1. Классификация методов криптографического преобразования информации

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.

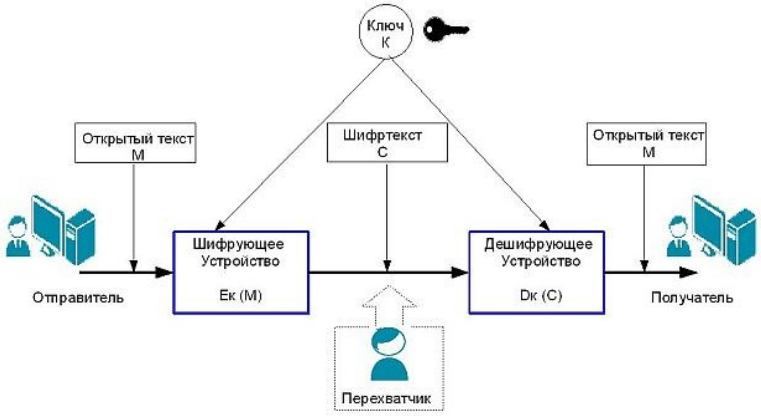


Рис. 2. Обобщённая схема криптографической системы

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

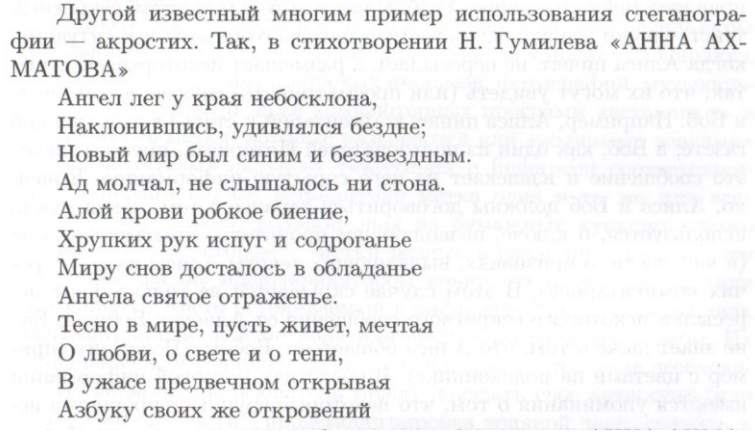
Классическая стеганография

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.

Компьютерная стеганография

Компьютерная стеганография - направление классической стеганографии, основанное на особенностях компьютерной платформы. Примеры:

• Использование зарезервированных полей компьютерных форматов файлов — суть метода состоит в том, что часть поля расширений, не заполненная информацией о расширении, по умолчанию заполняется нулями. Соответственно мы можем использовать эту «нулевую» часть для записи своих данных. Недостатком этого метода является низкая степень скрытности и малый объём передаваемой информации.

• Метод использования особых свойств полей форматов, которые не отображаются на экране — этот метод основан на специальных «невидимых» полях для получения сносок, указателей. К примеру, написание чёрным шрифтом на чёрном фоне. Недостатки: маленькая производительность, небольшой объём передаваемой информации.

• Использование особенностей файловых систем — при хранении на жестком диске файл всегда занимает целое число кластеров. Кластер имеет стандартный размер, например, 4 Кб. Соответственно, для хранения 1 Кб информации на диске выделяется 4 Кб информации, из которых 1Кб нужен для хранения сохраняемого файла, а остальные 3 ни на что не используются — соответственно их можно использовать для хранения скрываемой информации. Недостаток данного метода: лёгкость обнаружения.

Цифровая стеганография

Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования; далее, при воспроизведении этих объек-

тов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

Пример 1

Изображение дерева со скрытым с помощью цифровой стеганографии в нём другим изображением. Изображение спрятано с помощью удаления всех, кроме двух младших битов.

Информационная война

Необходимо подчеркнуть, что информационные войны велись сотни и тысячи лет назад. Хорошим примером может послужить Троянская война. Десять лет неприступная Троя сопротивлялась греческим войнам и была повержена с помощью троянского коня. Это был один из эффективных приемов информационной войны, примененный более 3000 лет назад.

Древний Египет часто вёл войны и проигрывал их, однако не переставал существовать как государство. Это указывает на то, что жрецами был выработан некий принцип на случай проигрыша в войне, который можно условно назвать «принципом культурного сотрудничества» со странами-победительницами.

Одно из первых задокументированных проявлений информационной войны было зафиксировано во время Крымской войны (1853—1856), когда сразу после Синопского сражения английские газеты в отчётах о сражении писали, что русские достреливали плававших в море раненых турок.

Вторая половина двадцатого века ознаменовалась появлением принципиально нового оружия - информационного. Соответственно возник и новый вид войны - информационная война. И если до рождения Интернета ведение информационной войны сильно ограничивалось доступом к СМИ, то с появлением всемирной сети, все естественные границы между "информационными территориями" исчезли, и "противоборствующие армии" получили возможность вторгаться на чужую землю и проводить боевые операции.

Информационная война – целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем.

Содержание практически не изменились: слухи, дезинформация, искажение фактов – все это присутствует. Но способы доведения информации кардинально отличаются. Сайт выступает в роли троянского коня, средство доставки – Интернет, различные глобальные телеканалы. На сегодняшний день создана глобальная информационная среда, так, в Китае зарегистрировано около 468 млн пользователей сети интернет, в России -около 50 млн пользователей. Практически за долю секунды информация любого содержания, как положительного, так и отрицательного появляется в этом глобальном поле.

Цель информационной войны - ослабить моральные и материальные силы противника или конкурента и усилить собственные. Она предусматривает меры пропагандистского влияния на сознание человека в идеологической и эмоциональной сферах. Очевидно, что информационная война - составная часть идеологической борьбы. Они не приводят непосредственно к кровопролитию, разрушениям, при их ведении нет жертв, никто не лишается пищи, крыши над головой. И

это порождает опасную беспечность в отношении к ним. Между тем, разрушения, которых наносят информационные войны в общественной психологии, психологии личности, по масштабам и по значению вполне соизмеримы, а порой и превышают последствия вооруженных войн.

Главная задача информационных войн заключается в манипулировании массами. Цель такой манипуляции зачастую заключается в:

- внесении в общественное и индивидуальное сознание враждебных, вредных идей и взглядов;
- дезориентации и дезинформации масс;
- ослаблении определенных убеждений, устоев;
- запугивании своего народа образом врага
- запугивании противника своим могуществом.

Чем более зависим противник от информационных систем при принятии решения, тем более он уязвим к вражескому манипулированию этими системами.

Таким образом, генеральная цель информационной войны - нарушить обмен информацией в лагере конкурента. Нетрудно понять, что этот вид оружия, как правило, вообще не направлен на задание потерь живой силе. В этом смысле кривая технологии вывела, наконец, к бескровной и в то же время исключительно эффективного оружия. Она уничтожает не население, а государственный механизм.

Основные черты информационной войны:

1. Такие войны, как правило, ведутся на чужой территории. Для них не существует ни границ, ни моральных ограничений. Из - за этого информационные атаки способны проникать даже в самые запретные тайники психики, поражая разум противника.

2. Информационная война не оставляет после себя следов. Человеку (или даже целому обществу) кажется, что он принимает самостоятельные решения, хотя на самом деле на него оказывается скрытое воздействие. По этой причине информационная атака становится особенно опасной: отразить ее очень трудно, не говоря уже о том, чтобы заранее к ней подготовиться.

3. Информационная война очень выгодна с экономической точки зрения. Для ее ведения не требуется больших материальных и людских ресурсов. Чтобы влиять на общественное мнение, достаточно минимального объема информации. Если она будет грамотно подана, это даст прекрасные результаты.

4. Особенности информационной войны определяются тем объектом, на который она направлена. В данном случае речь идет о человеческом мышлении. Если разрушение моста требует «жестких» методов, то в случае с информацией вполне можно обойтись и «мягкими» подходами.

5. Для информационной войны характерно подражание тому объекту, на который направлено ее основное воздействие. Это означает, что одна и та же информация может быть подана поразному для специализированных учреждений и для конкретного человека. Благодаря этому достигается «незаметность» целенаправленного информационного влияния, которое удачно «маскируется» под правду, а потому его трудно обнаружить .

6. Информационная война ставит перед собой цель изменить мировоззрение большой социальной группы или целого общества. Чтобы это произошло, «нападающая сторона» должна вникнуть в представления о мире своего противника, стать на его уровень мышления.

7. В информационной войне не задействуются психоактивные вещества, прямой шантаж и запугивание, подкуп, физическое воздействие и т. п. Хотя указанные воздействия могут применяться параллельно с информационной войной, они не являются обязательным элементом.

8. Информационное воздействие может осуществляться как на фоне информационного шума, так и в условиях информационного вакуума.

9. Средствами ведения информационной войны являются любые средства передачи информации — от СМИ до почты и сплетен.Наша жизнь во многом зависит от компьютеров и Интернета. Люди пользуются компьютерами в самых разнообразных целях – от переписки по элек-

тронной почте, общения в чатах и обмена фотографиями до ведения банковских дел, осуществления инвестиций, совершения покупок и планирования отпуска. Правительства, вооруженные силы, деловые круги и организации национальной безопасности также зависят от компьютерных сетей. Эта зависимость от Интернета спровоцировала целое множество угроз в киберпространстве.

Методы ведения информационных войн

Как правило, методами информационной войны является выброс дезинформации, или представление информации в выгодном для себя ключе. Данные методы позволяют изменять оценку происходящего населением территории противника, развивать пораженческое настроение, и, в перспективе, обеспечить переход на сторону ведущего информационное воздействие.

В качестве примера можно привести «прелестные письма», в которых Степан Разин призывал всех ищущих воли на свою сторону, выдавая себя за восстановителя справедливости, борца с предавшей царя местной властью. С появлением средств массовой информации и общим повышением уровня грамотности в XX веке ведение информационной войны стало более эффективным. Ярким примером изменения общественного сознания является деятельность Йозефа Геббельса, рейхсминистра народного просвещения и пропаганды.

Холодная война

Примером информационной войны считается Холодная война 1946—1991 годов (точнее, её идеологический аспект). Часть исследователей считает, что распад СССР был обусловлен не только амбициями республиканских элит и экономическими причинами, но и применением странами Запада информационных методов, которые способствовали началу внутриполитических процессов (возможно, что и вызвали их), закончившихся перестройкой и распадом СССР.

КГБ СССР осуществлял так называемые «активные мероприятия» по воздействию на зарубежное общественное мнение, а также на действия отдельных лиц, государственных и общественных организаций.

Наше время

Примером информационной войны также считаются и «информационно-психологические операции» (термин среди военных США), которые проводит Министерство обороны США в наше время, к примеру, в Ираке.

«Минобороны США заплатит частным подрядчикам в Ираке до 300 млн долларов за производство политических материалов, новостей, развлекательных программ и социальной рекламы для иракских СМИ, чтобы привлечь местное население к поддержке США», — пишет в 03 октября 2008 газета The Washington Post.

Ярким примером информационной войны является конфликт Израиля и Палестины, который является глобальным, поскольку затрагивает интересы более десятка стран. Противоборствующие стороны используют в своих интересах разнообразные информационные ресурсы: печатную прессу, телевидение, радио, интернет. Активно в информационной борьбе используются хакерские атаки, так израильская организация JIDF – «Еврейские силы интернет-обороны» – заблокировала действие интернет-сообщества «Израиль не страна!», размещенное в социальной сети Facebook и насчитывающее более 45 тысяч пользователей, а группа израильских хакеров «Gilad Team», взломавших более 15 сайтов, разместила на их страницах израильский флаг и слоган «Взломано» [12]. В свою очередь пропалестинские хакеры во время операции «Литой свинец» взломали несколько тысяч израильских сайтов, как сообщало информационное агентство Ynet, более 750 израильских сайтов были взломаны за первые сутки военного столкновения.

В ходе гражданской войны в Анголе в феврале 1988 года кубинской ПВО был сбит южноафриканский истребитель-бомбардировщик. Его обломки впоследствии выдавались за обломки многих других самолётов, о сбитии которых заявляли кубинцы.

Во время военной операции НАТО против Югославии в 1999 году югославские СМИ незадолго до прекращения бомбардировок сообщали о том, что ПВО страны уничтожила более 160 натовских самолётов и вертолётов. Сразу после прекращения бомбардировок начальник югослав-

ского генштаба Драголюб Ойданич объявил о 68 сбитых самолётах и вертолётах, а год спустя эта цифра была уменьшена до 37 самолётов и вертолётов.

Грузино-осетинский конфликт 2008 года

Информационная война также шла во время грузино-осетинского конфликта в августе 2008 года. Так Михаил Саакашвили поначалу заявлял: «На нашу территорию вторглись более 80 тысяч солдат, было введено более трех тысяч единиц бронетехники и еще около тысячи бронемашин стояло у наших границ. Наши территории бомбили несколько десятков, а может, и сотен самолетов, которые совершили более 200 боевых вылетов. Реально это была попытка искоренения и уничтожения нашего народа», что не соответствовало действительности (Южная Осетия - 3 тыс. личного состава и не меньше 20 танков и 25 САУ, Абхазия - 5 тыс. личного состава, контингент России - 15 тыс. личного состава)

В ноябре 2008 года на заседании временной парламентской комиссии по изучению августовских событий Михаил Саакашвили утверждал, что против Грузии «*воевали 95 % боеспособных частей вооруженных сил России*», при этом, по словам М. Саакашвили, грузинской армией было «*сбито 17-19 летательных аппаратов. 58-я российская армия фактических была сожжена 4-й грузинской бригадой*», в связи с чем «*... после уничтожения 58-й армии Россия .. выпустила более половины запаса своих „Искандеров“*».

Впоследствии Михаил Саакашвилли заявлял, что «*до сегодняшнего дня многие европейцы не понимают, как могли вообще грузины даже подумать о том, что за независимость стоит бороться против 3 тысяч танков, 20 самолетов, 80 тысяч вошедших иноземцев, но если бы в нас не было боевого гена, если бы у нас не было боевых способностей, тогда мы и не существовали бы*».Также М. Саакашвилли выразил благодарность сенатору Маккейну за то, что тот «*остановил своей деятельностью многие тысячи танков*». Чуть ранее Саакашвили заявлял, что «*Россия желала уничтожить Грузию и расчленить моё тело*».

В ходе конфликта и сразу после него российские и южноосетинские представители заявляли, что в Южной Осетии погибло более 2000 мирных жителей, впоследствии Следственному комитету при прокуратуре Российской Федерации удалось документально подтвердить гибель лишь 162 мирных жителей.

Американские специалисты по компьютерным технологиям неоднократно отмечали, что на сайт президента Грузии шла продолжительная кибератака со стороны России в виде увеличения "ложного" траффика в соотношении 5000:1, что приводило к значительному замедлению и остановке работы сервера. Также была проведена атака на сайт парламента Грузии, где были размещены изображения Саакашвили, напоминавшие Адольфа Гитлера.

Доктор социологических наук Козырев Г.И. в работе посвященной «*конструированию «жертвы» как способа создания управляемой конфликтной ситуации*» пишет, что западные политики и подконтрольные им СМИ пытались представить Грузию "*жертвой агрессии*", подвергшейся нападению со стороны России. Но эти события были лишь кульминацией длительного и сложного процесса конструирования из Грузии "жертвы", который осуществляли США и их союзники. Козырев делает сравнение с произошедшей ранее подобной операцией по конструированию "*жертвы*" из косовских албанцев, которая была проведена в Сербском крае Косово. Целенаправленное конструирование из Грузии "*жертвы-страны*", пишет автор, по сути, началось с приходом к власти президента М. Саакашвили. Периодически инициируемые грузинской стороной провокации в отношении российских миротворцев интерпретировались западными СМИ как посягательство "*большой и кровожадной*" России на "*маленькую, но гордую, демократическую*" Грузию. То есть, шла подготовка мирового общественного мнения к тому, что Россия является потенциальным агрессором, а Грузия - "*жертвой*".

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Практическое занятие. Оценочный расчет защищенности помещения от утечки речевых сообщений по акустическому каналу

Цель. Изучить содержание темы по методическим указаниям. В соответствии со схемой (рис. 1) рассчитать суммарную разборчивость формант в смежном помещении, коридоре и за

наружной стеной. Сделать выводы о возможности или невозможности утечки звуковой информации. Ответить на вопросы.

Пример расчетов по определению возможности утечки речевых сообщений

Рассмотрим возможность утечки речевых сообщений из исследуемого кабинета (рис. 1).

Исходные данные расчетов:

а) смежная комната: предельный спектр шумов - **ПС**-35 ; перегородка одинарная из досок ;

б) внутренний двор здания: предельный спектр шумов - **ПС**-45; стена из кирпичной кладки; окно занимает 40% стены;

в) коридор: предельный спектр шумов - **ПС**-40; стена из кирпичной кладки; дверь занимает 20% стены;

г) уровень интенсивности речи в октавных полосах берется из таблицы.

Порядок расчета.

1. Смежная комната.

По формуле определяем: $\mathbf{L}_2 = \mathbf{L}_1 + 6 - \mathbf{Q}_{пер}$,

где $\mathbf{L}_2$ - уровень речевого сигнала за звукоизолирующей перегородкой;

$\mathbf{L}_1$ - уровень речевого сигнала в контролируемом помещении.

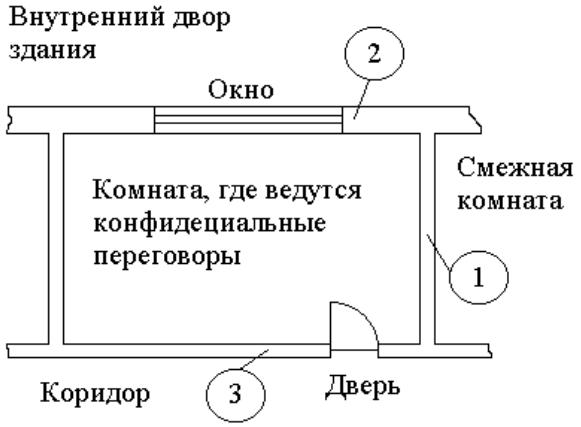


Рис. 1. Схема исследуемого кабинета

Значение $\mathbf{L}_1$ в октавных полосах будем определять, исходя из суммарного уровня речи 71 дБ. Значение $\mathbf{Q}_{пер}$ берем в таблице.

Номер октавы	Ср. частота, $f_р$	Уровни речи Речь, **L**1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ $\mathbf{Q}_{пер}$	**L**1 + 6 - $\mathbf{Q}_{пер}$, дБ	**L**2 = **L**р, дБ
1.	250	67,9	39-6	67,9 + 6 - (39 - 6)	40,9
2.	500	66,9	39	66,9 + 6 - 39	33,9
3.	1000	61,5	39	61,5 + 6 -39	28,5
4.	2000	57,0	39	57,0 + 6 - 39	24,0
5.	4000	53,0	39+6	53,0 + 6 - (39 + 6)	14,0
6.	6000	48,5	39+6	48,5 + 6 - (39 + 6)	9,5

Уровень ощущения формант $\mathbf{E}_ф$ определяется из выражения: **E**ф= **L**р – **L**ш.

Номер октавы	Ср. частота, fр	**L**2 = **L**р, дБ	Предельные спектры шумов ПС-35, **L**ш, дБ	**E**ф= **L**р – **L**ш, дБ	Значения коэф. разборчивости wi
1.	250	40,9	45	-4,1	0,095
2.	500	33,9	39	-5,1	0,075
3.	1000	28,5	35	-6,5	0,06
4.	2000	24,0	32	-8	0,04
5.	4000	14,0	30	-16	0
6.	6000	9,5	28	-18,5	0

По формуле находим суммарную разборчивость формант:

А ф.русск.= 0,05*(1,34w1 + 2,5 w2 + 4,24w3 +5,88 w4+5w5+1,04w6) =

= 0,05*(1,34x0,095 + 2,5x0,075 + 4,24x0,06 + 5,88x0,004) = 0,04 или (4%)

Выводы: расчетная суммарная разборчивость формант **А**ф.русск. <15%, смысл разговора в смежной комнате будет непонятен.

2. Внешняя стена

По формуле определяем величину звукоизоляции неоднородной перегородки, которыми являются внешняя стена и окно:

Qпер = **Q**1-10***lg***[1+(**S**o/(**S**1 + **S**o))*($10^{0,1(Q1-Qo)}$-1)],

где **Q**1 = 59 дБ;

Qo = 38 дБ;

(**S**o/(**S**1 + **S**o)) = 0,4.

Qпер = 59-10***lg***[1+0,4*($10^{0,1(59-38)}$-1)] = 42 Дб.

Уменьшение звукоизоляции стены с окном составило 17 дБ.

Дальнейшие вычисления проводим аналогично с п.1.

Номер октавы	Ср. частота, ***f***р	Уровни речи Речь, **L**1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ **Q**пер	**L**1 + 6 - **Q**пер, дБ	**L**2 = **L**р, дБ
1.	250	67,9	42-6	67,9 + 6 - (42 - 6)	37,9
2.	500	66,9	42	66,9 + 6 - 42	30,9
3.	1000	61,5	42	61,5 + 6 -42	25,5
4.	2000	57,0	42	57,0 + 6 - 42	21,0
5.	4000	53,0	42+6	53,0 + 6 - (42 + 6)	11,0
6.	6000	48,5	42+6	48,5 + 6 - (42 + 6)	6,5

Уровень ощущения формант **Е**ф определяется из выражения: **Е**ф= **L**р – **L**ш.

Номер октавы	Ср. частота, ***f***р	**L**2 = **L**р, дБ	Предельные спектры шумов ПС-45, **L**ш, дБ	**Е**ф= **L**р – **L**ш, дБ	Значения коэф. разборчивости ***w***i
1.	250	37,9	54	-16,1	0
2.	500	30,9	49	-18,1	0
3.	1000	25,5	45	-19,5	0
4.	2000	21,0	42	-21,0	0
5.	4000	11,0	40	-29,0	0
6.	6000	6,5	38	-31,5	0

По формуле находим суммарную разборчивость формант А ф.русск.= 0 (0%).

Выводы: расчетная суммарная разборчивость формант Аф.русск. < 15%, смысл разговора за окном не будет понятен.

3. Коридор

По формуле определяем величину звукоизоляции неоднородной перегородки, которыми являются внутренняя стена и дверь:

Qпер = **Q**1-10***lg***[1+(**S**o/(**S**1 + **S**o))*($10^{0,1(Q1-Qo)}$-1)],

где **Q**1 = 48 дБ;

Qo = 18 дБ;

(**S**o/(**S**1 + **S**o)) = 0,2.

Qпер = 59-10***lg***[1+0,2*($10^{0,1(48-18)}$-1)] = 25 дБ

Уменьшение звукоизоляции стены с дверью составило 23 дБ.

Дальнейшие вычисления проводим аналогично с п.1.

№ октавы	Ср. частота, ***f***р	Уровни речи Речь,**L**1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ **Q**пер	**L**1 + 6 - **Q**пер, дБ	**L**2 = **L**р, дБ
1.	250	67,9	25-6	67,9 + 6 - (25 - 6)	54,9

2.	500	66,9	25	66,9 + 6 - 25	47,9
3.	1000	61,5	25	61,5 + 6 - 25	42,5
4.	2000	57,0	25	57,0 + 6 - 25	38
5.	4000	53,0	25+6	53,0 + 6 - (25 + 6)	28
6.	6000	48,5	25+6	48,5 + 6 - (25 + 6)	23,5

Уровень ощущения формант **Е**ф определяется из выражения: **Е**ф= **L**р – **L**ш.

№ октавы	Ср. частота, *f*р	**L**2 = **L**р, дБ	Предельные спектры шумов ПС-40, **L**ш, дБ	**Е**ф= **L**р – **L**ш, дБ	Значения коэффициентов разборчивости *w*i по табл. 3
1.	250	54,9	49	5,9	0,4
2.	500	47,9	44	3,9	0,35
3.	1000	42,5	40	2,5	0,3
4.	2000	38	37	1	0,25
5.	4000	28	35	-7	0,05
6.	6000	23,5	33	-9,5	0,03

По формуле находим суммарную разборчивость формант

А ф.русск.= 0,05*(1,34*w*1 + 2,5 *w*2 + 4,24*w*3 +5,88 *w*4+5*w*5+1,04*w*6) =

= 0,05*(1,34x0,4 + 2,5x0,35 + 4,24x0,3 + 5,88x0,25 +

+ 5,0x0,05 + 1,04x0,03) = 0,22 (22%).

Выводы: расчетная суммарная разборчивость формант Аф.русск. = 22%. Смысл разговора за дверью будет понятен, слышимость удовлетворительная. Необходимо обеспечить звуковую изоляцию стены и двери.

Вопросы.

1. Что такое разборчивость?
2. Какая бывает разборчивость?
3. От чего зависит восприятие речи?
4. Какие акустические помехи вы знаете.
5. Что такое речевой шум?
6. Что оказывает влияние на разборчивость речевых сообщений?
7. Как вы понимаете эффект реверберации.

Практическое занятие 2. Оценочный расчет защищенности помещений от утечки информации по электромагнитному каналу.

Цель. Произвести расчет защищенности помещения от утечки информации по электромагнитному каналу.

Задание

1. В соответствии со схемой (рис. 2) произвести расчеты защищенности помещения от утечки информации по электромагнитному каналу.

Среднеквадратические значения напряженности поля $\mathbf{E}_a$ атмосферных помех не расчитывать, считать одинаковыми для всех вариантов и равными:

	100 МГц	500 МГц	1000 МГц
$\mathbf{E}_a$, мкВ/м ($\mathbf{T}_a$=293^{o}K, *f*экв=40 Мгц)	0,346	1,738	3,467

Приведем пример расчета защищенности помещения от утечки информации по электромагнитному каналу. В качестве источника электромагнитного излучения возьмем ПЭВМ, расположенную на некотором удалении от контролируемой зоны (рис.2).

Пример расчета.

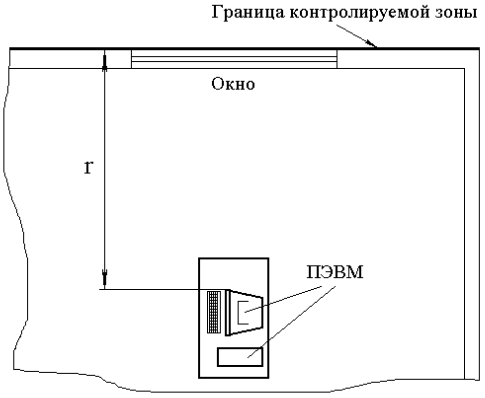


Рис. 2. Схема помещения для проведения расчетов

Таблица 2

Значения напряженности электромагнитного поля **E**, создаваемого ПЭВМ

Номер п/п	Значения электромагнитного поля **E** (мкВ/м) на частотах		
	100 МГц	500 МГц	1000 МГц
1.	630	1400	1400
2.	610	1370	1390
3.	620	1420	1400
4.	610	1360	1400
5.	600	1360	1390
6.	630	1410	1400

Исходные данные.

В помещении расположена ПЭВМ (рис.2), на которой обрабатываются конфидециальные данные. Расстояни от ПЭВМ до контролируемой зоны составляет r = 15 м. Граница контролируемой зоны проходит по периметру железобетонной стены толщиной 160 мм, в стене имеется оконный проем, не превыщающий 30% площади стены. Окно закрыто металлической решеткой с ячейкой 5 см. Значения напряженности электромагнитного поля **E**, создаваемого ПЭВМ на частотах 100 МГц, 500МГц и 1000 МГц, берем из табл. 2, п. 6. При определении коэффициента затухания принимаем **n**=1,4. В качестве кретерия защищенности помещения от утечки информации на границе контролируемой зоны отношение сигнал / шум принимаем равным $\Delta \leq 1$.

Результаты расчета сводим в таблицу:

Ход вычислений	Данные, полученные из таблиц или в результате расчетов, на частотах		
	100 МГц	500 МГц	1000 МГц
Из табл. 2, п. 6 выбираем значения электромагнитного поля **E**, создаваемого ПЭВМ, мкВ/м	610	1370	1390
Определяем коэффициент затухания по формуле $\mathbf{k}_з = 1 / \mathbf{r}^n$, **r** = 15, **n** = 1,4	0,0226		
Выбираем из табл. 2, п. 6 максимальные значения коэффициента экранирования $\mathbf{k}_{экр}$	39,8	22,4	17,8
Определяем напряженность электромагнитного поля на границе контролируемой зоны по формуле (2) $\mathbf{E}_{кз} = \mathbf{E}^* \mathbf{k}_з * \mathbf{k}_{экр}$, мкВ/м	0,346	1,38	1,76
Определяем среднеквадратическое значение напряженности поля $\mathbf{E}_a$ атмосферных помех по формуле (1), принимая $\mathbf{T}_a = 293^oK$, $f_{экв}$=40 МГц	0,346	1,738	3,467
Определяем отношение сигнал/шум на границе контролируемой зоны по формуле $\Delta = \mathbf{E}_{кз} / \mathbf{E}_a$	0,999≈1	0,79	0,51

Расчеты показали, что на всех частотах значение $\Delta \leq 1$. Следовательно, расстояние до границы контролируемой зоны достаточно для обеспечения безопасности сообщений, излучаемых в

окружающее пространство ПЭВМ. Дополнительных мер по обеспечению защиты помещения от утечки информации не требуется.

Варианты:

Номер варианта	$k_з = 1 / r^n$		$k_{экр}$ Таб. 1, пункт	E Таб. 2, пункт	Δ
	r	n			
1.	15	1,3	1	1	1
2.	20	1,4	2	2	1
3.	15	1,5	3	3	1
4.	20	1,6	4	4	1
5.	15	1,7	5	5	1
6.	20	1,8	6	6	1
7.	15	1,4	1	2	1
8.	20	1,5	2	3	1
9.	15	1,6	3	4	1
10.	20	1,7	4	5	1
11.	15	1,8	5	6	1
12.	20	1,3	6	1	0,7
13.	15	1,5	1	3	0,7
14.	20	1,6	2	4	0,7
15.	15	1,7	3	5	0,7
16.	20	1,8	4	6	0,7
17.	15	1,3	5	1	0,7
18.	20	1,4	6	2	0,7
19.	15	1,6	1	4	0,7
20.	20	1,7	2	5	0,7
21.	15	1,8	3	6	0,7

2. По заданным значениям **Δ** рассчитать **r** для частот 100, 500 и 1000 МГц.

Практическое занятие 3. Изучение традиционных симметричных криптосистем. Шифры перестановок.

Цель: Целью выполнения занятия 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. 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**

До перестановки

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**

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
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 ДО-	

Номер варианта	Текст	Ключевое слов
	СТУП 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
21.	УГРОЗА ЦЕЛОСТНОСТИ ВКЛЮЧАЕТ В СЕБЯ ЛЮБОЕ УМЫШЛЕННОЕ ИЗМЕНЕНИЕ ДАННЫХ, ХРАНЯЩИХСЯ В ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ ИЛИ ПЕРЕДАВАЕМЫХ ИЗ ОДНОЙ СИСТЕМЫ В ДРУГУЮ	ОТНОШЕНИЕ

Контрольные вопросы.

1. Приведите примеры шифров перестановки.
2. Сформулируйте общие принципы для методов шифрования подстановкой.
3. Опишите алгоритм любого метода шифрования перестановкой. Приведите пример шифрования некоторого сообщения этим методом. Каков алгоритм расшифрования в этом методе?

4. Каким образом можно зашифровать и расшифровать сообщение методом табличной перестановки, если размер шифруемого сообщения не кратен размеру блока

Практическое занятие 4. Изучение традиционных симметричных криптосистем Шифры замены.

Цель: Целью – 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
21.	ЕСЛИ АТАКА НЕ УДАЛАСЬ, ХАКЕР СТАРАЕТСЯ ОСТАВИТЬ ЛОЖНЫЙ СЛЕД	ВПАДИНА

Контрольные вопросы.

1. В чем заключаются многоалфавитные подстановки?
2. Приведите пример шифра одноалфавитной замены.
3. К какой группе методов шифрования с закрытым ключом относится метод с использованием таблицы Вижинера?
4. Каковы алгоритмы шифрования и расшифрования в методе Вижинера? Приведите пример шифрования некоторого сообщения этим методом.

Практическое занятие 5. Количественная оценка стойкости парольной защиты

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.

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

$S^* = [V \cdot P / T]$, (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:

$S^* \le S = A^L$. (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
21	10^{-4}	20 паролей/мин	2 недели
22	10^{-5}	15 паролей/мин	10 дней
23	10^{-6}	3 паролей/мин	5 дней

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. В первом случае она выполняется на учебных занятиях под руководством преподавателя и по его заданию. Студенты обеспечиваются необходимым учебным материалом и дидактическими материалами.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя, но без его непосредственного участия. Видами заданий для внеаудиторной работы являются: изучение текста учебной литературы, конспектирование текста, работа с конспектом лекции, ответы на контрольные вопросы при выполнении индивидуального задания, тестирование, решение задач, продумывание алгоритма будущей программы, работа с компьютером, а именно, кодирование и отладка программы, подготовка отчета по лабораторным заданиям, подготовка к сдаче экзамена.

Основные формы самостоятельной учебной работы:

работа над конспектом лекции: лекции – основной источник информации по многим предметам, позволяющий не только изучить материал, но и получить представление о наличии других источников, сопоставить разные взгляды на основные проблемы данного курса. Лекции предоставляют возможность «интерактивного» обучения, когда есть возможность задавать преподавателю вопросы и получать на них ответы. Поэтому имеет смысл находить время для хотя бы бегло-

го просмотра информации по материалу лекций (учебники, справочники и пр.) и непонятные, а также дискуссионные моменты обсуждать с преподавателем, другими студентами;

подготовка к практическому занятию: производится, как правило, с использованием методических пособий, состоит в теоретической подготовке (особенно для семинаров) и выполнении практических заданий (решение задач, ответы на вопросы и т.д.).

Существует ряд форм практических занятий:

- лабораторные занятия с оборудованием (иногда с постановкой опытов);
- практикум по освоению тех или иных навыков, методик;
- семинар (с разбором теоретических вопросов в рамках какой-либо темы);
- коллоквиум (семинар но итогам изучения нескольких родственных тем); □

подготовка к семинарскому занятию производится по правилам выполнения задания практической работы, обычно по определенному вопросу и более или менее узкому кругу литературы (часто всего два-три учебных пособия);

доработка конспекта лекции с применением учебника, методической литературы, дополнительной литературы: этот вид самостоятельной работы студентов особенно важен в том случае, когда изучаемый предмет содержит много неоднозначно трактуемых вопросов, проблем. Тогда преподаватель заведомо не может успеть изложить различные точки зрения, и студент должен ознакомиться с ними по имеющейся литературе.

Кроме того, рабочая программа предметов предполагает рассмотрение некоторых относительно несложных тем только во время самостоятельных занятий, без чтения лектором; подбор, изучение, анализ и конспектирование рекомендованной литературы; самостоятельное изучение отдельных тем, параграфов; консультации по сложным, непонятным вопросам лекций, семинаров, зачетов;

подготовка к зачету: данная форма СРС может быть весьма разнообразной по своей сути, так как сам зачет бывает различным. Он проводится обычно по итогам семестра перед сессией в письменной или устной форме, причем преподаватель может включать в него вопросы как практических занятий, так и лекционных (что особенно уместно, когда по данному предмету не сдается экзамен).

Главное отличие зачета от экзамена – почти всегда не пяти-, а двухбалльная система оценки (сдал – не сдал), что делает его получение несколько более простым делом. С другой стороны, порой процедура его сдачи достаточно сложна, а иногда применяется и пятибалльная оценка (так называемый дифференцированный зачет).

Таким образом, для сдачи зачета необходимо, прежде всего, выполнить все требования преподавателя, что предполагает знание этих требований. Нужно как можно раньше выяснить, какие вопросы предстоит готовить и каковы правила самой процедуры (учитывается ли посещаемость, надо ли пропущенные занятия отрабатывать, а если надо, то каким образом и т.д.). Практика показывает, что хорошее посещение занятий является почти полной гарантией получения зачета, так как тогда можно быть в курсе всех требований преподавателя. И, напротив, большое количество пропусков может осложнить жизнь даже сильному студенту.

Кроме того, необходимо учитывать, что проблемы могут появиться при распространенном подходе студента к практическим занятиям, когда многие работают первые месяцы вполсилы, накапливая задолженности по выполнению рефератов, практических заданий, конспектов и пр., а перед сессией пытаются все это сделать за одну неделю. Старайтесь распределять силы равномерно по всей дистанции семестра, и тогда зачетная неделя перед сессией будет не самой напряженной, а самой разгрузочной.

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.

СОДЕРЖАНИЕ