МИНИСТЕРСТВО ОБРАЗОВАНИЯ АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ

АЗЕРБАЙДЖАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

"ЦЕНТР ПО ПОДГОТОВКЕ МАГИСТРОВ"

Шихлар Нигяр Каир гызы

(ф.и.о. магистра)

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему: "Проблемы надежности в сетях и защита информации"

Шифр и название направления: **İİM060509** **"Компьютерные науки"**

Шифр и название специальности: **“Экономические информационные системы”**

Научный руководитель: **доц., к.т.н., А.М.Байрамов**

Руководитель магистерской программы: **д.э.н.,проф. Я.Р.Абдуллаев**

Заведующий кафедры: **доц., к.т.н. А.М. Байрамов**

Б А К У - 2 0 1 5

Оглавление

Введение

Научно-технический прогресс и связанная с ним интеграция человеческой деятельности привели к возникновению глобальных проблем современности, которые остро поставили перед человеческой цивилизацией проблему выживания, безопасности ее развития.

В зависимости от угроз человеческому существованию можно рассматривать следующие составляющие безопасности человеческого общества: ядерную, экологическую, политическую, технологическую, экономическую и другие. Основой этих составляющих является ***информационная безопасность***.

Ряд вопросов возникает после того, как возникает необходимость обеспечения той или иной комбинации требований для работы в глобальных сетях. Какие программно-аппаратные средства и организационные меры должны быть реализованы? Каков профиль риска? Основа ответов на подобные вопросы - это концептуальная политика безопасности для организации.

Политики безопасности можно разделить на две категории - технические политики, реализуемые с помощью оборудования и программ, и административные политики - выполняемые людьми, использующими систему и людьми, управляющими ей.

В течении многих лет в организациях преобладали локальные вычислительные сети (ЛВС), с функциями совместного использования данных, подключения к сети дополнительных устройств, например принтера. Далее ЛВС объединялись друг с другом, в результате появился новый тип - так называемые территориальные распределенные сети (ТРС). Эти сети

позволяют осуществлять обмен информацией внутри географически разрозненных организаций.

В настоящее время существует большое количество ИВС оп, среди которых наиболее известны **Internet, Relcom, Sovintel,** кроме того специализированные сети “ЛУКойл- Западная Сибирь”, Medical Systems, сеть ВУЗов Северо–Западного региона.

Глобальной информационной супермагистралью, призванной связать разрозненные компьютерные системы является ИВС оп Internet. Первоначально созданная как сеть ARPANET, после чего национальный научный фонд США для соединения в сеть большого числа научно-исследовательских учреждений и развития международной кооперации учредил проект NSFNET. С 1990 года сеть ARPANET прекратила свое существование, а сеть Internet распространилась за пределы академического мира; предложив обществу одновременно доступ к информации и быстрое глобальное средство связи. Компьютеры, включенные в сеть могут использовать одну из следующих операционных систем: Windows-9X, NT, NetWare, OS/2, Mac OS, UNIX. Скорость обмена данными зависит от многих условий, среди которых конфигурация компьютера, сети, навыки пользователей. Обмен данными осуществляется с помощью Web–браузера у клиента, сетевых протоколов (TCP/IP) и сервера HTTP (Hyper-Text Transfer Protocol).

В Internet идя на встречу потребителям провайдеры (коммерческая служба обеспечивающая своим абонентам доступ к Internet), предлагают пользователям безопасные каналы передачи данных, снабженные комбинацией туннельных и шифрующих маршрутизаторов. Аутентификация пользователя производится с помощью специальных защитных маркеров, работающих по принципу “запрос-пароль”, причем надежность составляет около 99,9 % для 12 и более сетевых узлов, при этом

задержка при передаче сообщений от отправителя к получателю не превышает 150 мс для территориально-распределенной сети.

С распространением письменности в человеческом обществе появилась потребность в обмене письмами и сообщениями, что, вызвало необходимость сокрытия содержимого письменных сообщений от посторонних. Методы сокрытия содержимого письменных сообщений можно разделить на три группы. К первой группе относятся методы маскировки или *стеганографии*, которые осуществляют сокрытие самого факта наличия сообщения; вторую группу составляют различные методы тайнописи или *криптографии* (от греческих слов ktyptos - тайный и grapho - пишу); методы третьей группы ориентированы на создание специальных технических устройств, засекречивания информации.

Диссертационная работа состоит из трёх глав. Первая глава работы посвящена изучению вопросов компьютерной безопасности.В этой же главе определен круг вопросов безопасности информационных систем.

Вторая глава посвящена вопросам построение зашиты сетей, а также изучению задачи контроля и протоколирования в этом же главе изучены вопросы вирусах методах зашита программных средств.

В третьей главе изучены вопросы применения новых методов и средств защиты информации и криптоанализа.

Работа закончивается с предложениям и списпом литературы.

Глава 1. Основные теории компьютерной безопасности.

1.1 Безопасность информационных систем.

Вопросы информационной безопасности занимают особое место и в связи с возрастающей ролью в жизни общества требуют к себе все большего внимания. Успех практически любой деятельности в немалой степени зависит от умения распоряжаться такой ценностью, как информация. В законе РФ «Об информации, информатизации и защите информации» подчеркивается, что «информационные ресурсы являются объектами собственности граждан, организаций, общественных объединений, государства».

Информационная безопасность – достаточно сложная и многогранная проблема, решение которой под силу хорошо организованным структурам и успех может принести только систематический, комплексный подход. Для решения данной проблемы рассматриваются меры ***законодательного, административного, процедурного и программно–технического уровня***.

Возникновение проблемы информационной безопасности во многом связано с созданием и повсеместным использованием ЭВМ и, на их основе, разнообразных организационно-технических ("человек-машина") систем. Важнейшим классом таких систем являются автоматизированные системы управления (АСУ), в которых сбор, хранение и обработка данных при реализации функций управления осуществляется средствами автоматизации и ВТ.

Современные АСУ объединяют в единый контур большое число разнородных территориально распределенных объектов и включают в себя специализированные и универсальные ЭВМ, устройства передачи данных, терминалы и другие абонентские устройства – информационно-вычислительные сети (ИВС). Создание АСУ и ИВС привело к

формированию в рамках мировой цивилизации международного информационного пространства. С другой стороны, повсеместное внедрение в практику человеческой деятельности систем управления сопровождается целым комплексом негативных последствий, таких как компьютерные преступления, экономические и политические диверсии с применением средств ИВС, электронные диверсии, нарушения прав и свобод личности и т.п. Все это свидетельствует об особой роли информационной безопасности в жизни человеческого общества.

Предметом защиты является информация, хранящаяся, обрабатываемая и передаваемая в компьютерных (информационных) системах. Особенностями данного вида информации являются:

- двоичное представление информации внутри системы, независимо от физической сущности носителей исходной информации;
- высокая степень автоматизации обработки и передачи информации;
- концентрация большого количества информации в КС.

Объектом защиты информации является компьютерная (информационная) система или автоматизированная система обработки информации (АСОИ).

Развитие теоретических основ создания и применения сложных систем управления существенно зависит от темпов развития **информатики** - комплекса наук, изучающих законы, методы и средства накопления, обработки и передачи информации с помощью ЭВМ и других технических средств. В то же время информатика является лишь обеспечивающим звеном в общей системе научных основ управления, которые опираются на теоретический фундамент **кибернетики**.

Теоретическим базисом информатики является теория информации, которая входит на правах самостоятельного раздела в кибернетику и включает методы математического описания и исследования информационных процессов различной природы, методы передачи,

обработки, хранения, извлечения и классификации информации в различных областях деятельности.

Создание любой АСУ невозможно без разработки и оптимизации алгоритмического обеспечения. Основой алгоритмического обеспечения является теория алгоритмов - раздел математики, изучающий процедуры (алгоритмы) вычислений и математические объекты, которые могут быть определены на базе методов теорий множеств, отношений и функционалов, вычислительных процедур и сложности алгоритмов.

Построение территориально распределенных систем управления предполагает необходимость исследования не только методов и алгоритмов обработки, накопления и хранения информации, но и методов ее передачи между элементами системы. Это обстоятельство обусловливает использование при исследовании и разработке автоматизированных систем управления методов теории передачи информации, теории кодирования и криптологии, являющихся разделами теории информации..

Совокупность этих теорий, хотя и охватывает различные области организации скрытной передачи данных в системах управления, тем не менее не позволяет структурировать проблему обеспечения безопасности информации и проводить анализ процессов во всех аспектах функционирования системы (морфологическом, функциональном, информационном и прагматическом). Поэтому возникает необходимость формирования нового научного направления - **теории обеспечения безопасности информации**, интегрирующей основные научные положения прикладной теории алгоритмов, теории передачи информации, теории кодирования, криптологии и с единых системных позиций изучающей методы предотвращения случайного или преднамеренного раскрытия, искажения или уничтожения хранимой, обрабатываемой и передаваемой информации в системах управления, функционирующих на базе средств

вычислительной техники. Роль и место в современной науке, а также основные научные направления данной теории показаны на рис.1.

В связи с тем, что новая теория появилась на основе синтеза методов нескольких разделов кибернетики и информатики, исследует информационные процессы, протекающие в организационно-технических системах, и ориентирована, прежде всего, на средства автоматизированной обработки данных, то по своему содержанию она должна входить в информатику в качестве самостоятельного раздела с четко обозначенной предметной областью.

В настоящее время понятие "информация" трактуется, пожалуй, наиболее широко - от философски обобщенного до бытового, в зависимости от целей, которые ставит перед собой автор. Так, В.И. Шаповалов дает такое определение: "***Информация*** об объекте есть изменение параметра наблюдателя, вызванное взаимодействием наблюдателя с объектом". С другой стороны, к определению информации существуют подходы, предложенные Шенноном и связанные с ее количественным измерением.

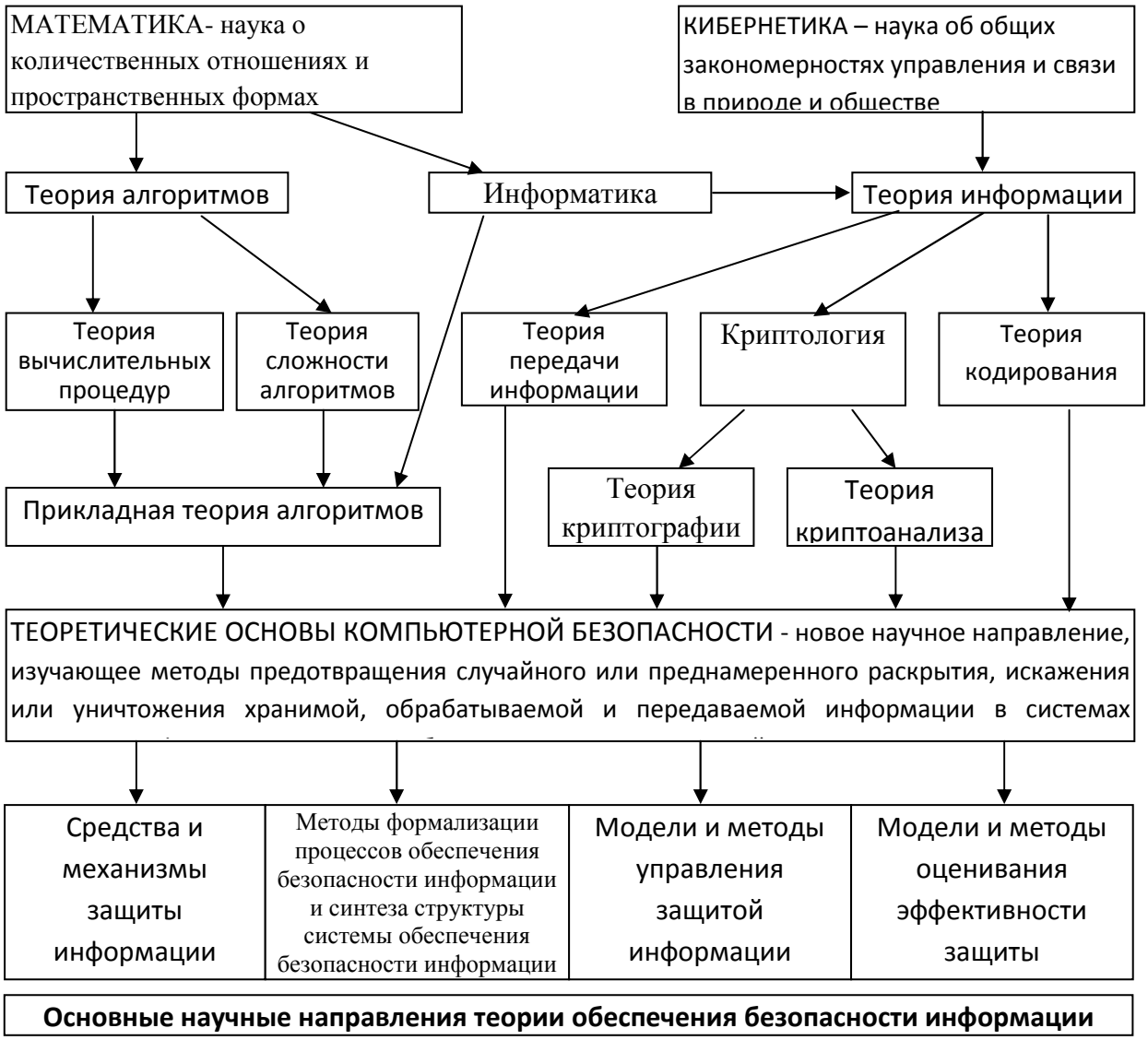
Под ***информацией*** будем понимать сведения: о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах, характеристиках) в некоторой предметной области, воспринимаемые человеком или специальным устройством и используемые (необходимые) для оптимизации принимаемых решений в процессе управления данными объектами. Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т.п.) на носителях различных типов. В связи с развивающимся процессом информатизации общества все большие объемы информации накапливаются, хранятся и обрабатываются в автоматизированных системах, построенных на основе современных средств вычислительной техники и связи.

Информация – сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), отраженные на

материальных носителях, используемые в целях получения знаний и практических решений.

Свойства информации:

- ***Ценность информации*** определяется степенью ее полезности для владельца (степенью обеспечением возможности достижения цели, поставленной перед получателем)**.**
- **Репрезентативность** – правильность отбора информации и формирования в целях адекватного отражения свойств объекта.
- **Достаточность (полнота)** информации – содержание минимального, но достаточного для принятия правильного решения состава (набора)



Основные научные направления теории обеспечения безопасности информации

- показателей.

- **Доступность** информации обеспечивается выполнением соответствующих процедур ее получения и преобразования.
- **Актуальность** информации - степень сохранения ценности информации для управления в момент ее использования, зависит от динамики ее изменения.

Законом РФ «Об информации, информатизации и защите информации» гарантируется право собственника информации на ее использование и защиту от доступа к ней других лиц (организаций). Если доступ к информации ограничен, то такая информация называется ***конфиденциальной***. Конфиденциальная информация может содержать государственную или коммерческую тайну.

Государственную тайну могут содержать сведения, принадлежащие государству (государственному учреждению). В соответствии с законом «О государственной тайне» сведениям, представляющим ценность для государства, может быть присвоена одна из трех возможных степеней (гриф) секретности: *«особая важность»*, *«совершенно секретно»* и *«секретно»*. Для менее важной информации в государственных учреждениях существует гриф *«для служебного пользования»*.

Коммерческую тайну могут содержать сведения, принадлежащие частному лицу, фирме, корпорации и т.д. Для обозначения ценности конфиденциальной коммерческой информации используют три категории: «*коммерческая тайна – строго конфиденциально (строгий учет)», «коммерческая тайна – конфиденциально», «коммерческая тайна»;*

- ***Достоверность информации (адекватность)*** определяется достаточной для владельца точностью отражать объекты и процессы окружающего мира в определенных временных и пространственных рамках.

- **Точность** информации определяется степенью близости получаемой информации к реальному состоянию объекта.

➢ **Устойчивость** информации отражает ее способность реагировать на изменения исходных данных без нарушения точности.

Информация, искаженно представляющая действительность, может нанести владельцу значительный материальный и моральный ущерб. Если информация искажена умышленно, то ее называют дезинформацией;

❖ ***Своевременность информации***, т.е. соответствие ценности и достоверности определенному временному периоду. Данное свойство определяется выражением:

$$C(t)=C_0e^{-2,3t/\tau},$$

где C_0 – ценность информации в момент ее возникновения, t – время от момента возникновения информации до момента определения ее стоимости, τ – время от момента возникновения информации до момента ее устаревания.

Информационная система – это организационно - упорядоченная совокупность информационных ресурсов, технических средств, технологий и персонала, реализующих информационные процессы в традиционном или автоматизированном режиме для удовлетворения информационных потребностей пользователей.

Продуктом информационной системы является ***информация***, свойства которой изменяются в соответствии с заданной технологией с помощью комплекса технических средств и людей, выполняющих определенные технологические операции. ***Технологические операции*** – это совокупность действий, направленных на изменение состояния информации, которая на выходе системы приводится к нужному виду и содержанию.

Источниками конфиденциальной информации в информационных системах являются люди, документы, публикации, технические носители, технические средства обработки информации, продукция, промышленные и производственные отходы.

В большинстве случаев активные действия противоборствующих сторон по сбору информации осознаны и целенаправленны. К ним относятся:

- разглашение конфиденциальной информации ее обладателем;
- утечка информации по различным (в основном-техническим) каналам;
- несанкционированный доступ к конфиденциальной информации различными способами .

Под ***автоматизированной системой обработки информации*** (АСОИ) понимают организационно-техническую систему, представляющую собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных (СВТ и связи);
- методов и алгоритмов обработки в виде программного обеспечения;
- информации (массивов, наборов, баз данных) на различных носителях;
- персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений.

Одной из особенностей обеспечения информационной безопасности в АС является то, что абстрактным понятиям, таким как "субъект доступа", "информация" и т.п., ставятся в соответствие физические представления в ЭВМ:

- для представления «субъектов доступа» - активные программы и процессы,
- для представления информации - машинные носители информации в виде внешних устройств компьютерных систем (терминалов, печатающих устройств, различных накопителей, линий и каналов связи), томов, разделов и подразделов томов, файлов, записей, полей записей, оперативной памяти и т.д.

Утечка информации – это бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена.

Утечка информации по своей сущности всегда предполагает противоправное (тайное или явное, осознанное или случайное) овладение конфиденциальной информацией, независимо от того, каким путем это достигается.

Утечка охраняемой информации может произойти при наличии ряда обстоятельств:

- есть злоумышленник, который такой информацией интересуется и затрачивает определенные силы и средства для ее получения;
- есть условия, при которых противник может рассчитывать на овладение интересующей его информацией.

Причины и условия утечки информации, при всех своих различиях, имеют много общего.

Причины связаны, как правило, с несовершенством норм по сохранению военных и государственных секретов, а также нарушением этих, отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и другими материалами, содержащими конфиденциальную информацию.

Условия включают различные факторы и обстоятельства, которые складываются в процессе научной, производственной, служебной, отчетной информацией и другой деятельности и создают предпосылки для утечки секретов. К таким факторам и обстоятельствам могут, например, относиться:

- недостаточное знание служащими организаций правил защиты военной и государственной тайны и непонимание (или недопонимание) необходимости их тщательного соблюдения;
- использование не аттестованных технических средств обработки конфиденциальной информации;

- слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами;
- текучесть кадров, в том числе владеющих сведениями, составляющими военную и государственную тайну.

Большая часть причин и условий, создающих предпосылки и возможность неправомерного овладения конфиденциальной информацией, возникает из-за недоработок руководителей организации и их сотрудников.

Кроме того, утечке информации способствуют:

- стихийные бедствия (шторм, ураган, землетрясение, наводнение);
- неблагоприятная внешняя среда (гроза, дождь, снег);
- катастрофы (пожар, взрывы);
- неисправности, отказы, аварии технических средств и оборудования.

Словосочетание *«информационная безопасность»* в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин "информационная безопасность" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Информационная безопасность АС - состояние рассматриваемой автоматизированной системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды.

В Законе РФ "Об участии в международном информационном обмене" информационная безопасность определяется аналогичным образом – как состояние защищенности информационной среды общества,

обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Под ***информационной безопасностью*** понимают защищенность *информации* и *поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

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

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления *субъектов информационных отношений* и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1. Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае "пусть лучше все сломается, чем враг узнает хоть один секретный бит", во втором – "да нет у нас никаких секретов, лишь бы все работало".

2. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например,

учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Согласно определению ИБ, она зависит не только от ЭВМ, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении ИБ перед существительным "ущерб" стоит прилагательное "неприемлемый". Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

1.2 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, выделим ее как важнейший элемент информационной безопасности. 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 можно подразделить на ***статическую*** (понимаемую как неизменность информационных объектов) и ***динамическую*** (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

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 Web-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. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы. Наконец, конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

1.3. Важность и сложность проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю – национальном, отраслевом, корпоративном или персональном.

Для иллюстрации обратимся к примерам.

- В **Доктрине информационной безопасности Российской Федерации** защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и

телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере.

- По распоряжению президента США Б. Клинтона (от 15 июля 1996 года, номер 13010) была создана Комиссия по защите критически важной инфраструктуры как от физических нападений, так и от атак, предпринятых с помощью информационного оружия. В начале октября 1997 года глава вышеупомянутой комиссии Роберт Марш заявил, что в настоящее время ни правительство, ни частный сектор не располагают средствами защиты от компьютерных атак, способных вывести из строя коммуникационные сети и сети энергоснабжения.

- Американский ракетный крейсер "Йорктаун" был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0. Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого ПО с целью снижения стоимости военной техники.

- Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, АР, 17 сентября 1996 года).

- Как сообщил журнал Internet Week от 23 марта 1998 года, потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности. Согласно результатам совместного исследования Института информационной безопасности и ФБР, в 1997 году ущерб от **компьютерных преступлений** достиг 136 миллионов долларов, что на 36% больше, чем в

1996 году. Каждое компьютерное преступление наносит ущерб примерно в 200 тысяч долларов.

- В середине июля 1996 года корпорация General Motors отозвала 292860 автомобилей марки Pontiac, Oldsmobile и Buick моделей 1996 и 1997 годов, поскольку ошибка в ПО двигателя могла привести к пожару.
- В феврале 2001 года двое бывших сотрудников компании Commerce One, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом.
- Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.

Понятно, что подобных примеров множество, можно вспомнить и другие случаи – недостатка в нарушениях ИБ нет и не предвидится. Чего стоит одна только "Проблема 2000" – стыд и позор программистского сообщества!

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что ИБ есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует быстрому

развитию средств обеспечения ИБ. Следует исходить из того, что необходимо конструировать надежные системы (информационной безопасности) с привлечением ненадежных компонентов (программ). В принципе, это возможно, но требует соблюдения определенных архитектурных принципов и контроля состояния защищенности на всем протяжении ***жизненного цикла ИС***.

Приведем еще несколько цифр. В марте 1999 года был опубликован очередной, четвертый по счету, годовой отчет "Компьютерная преступность и безопасность-1999: проблемы и тенденции" (Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey). В отчете отмечается резкий рост числа обращений в правоохранительные органы по поводу компьютерных преступлений (32% из числа опрошенных); 30% респондентов сообщили о том, что их информационные системы были взломаны внешними злоумышленниками; атакам через Internet подвергались 57% опрошенных; в 55% случаях отмечались нарушения со стороны собственных сотрудников. Примечательно, что 33% респондентов на вопрос "были ли взломаны ваши Web-серверы и системы электронной коммерции за последние 12 месяцев?" ответили "не знаю".

В аналогичном отчете, опубликованном в апреле 2002 года, цифры изменились, но тенденция осталась прежней: 90% респондентов (преимущественно из крупных компаний и правительственных структур) сообщили, что за последние 12 месяцев в их организациях имели место нарушения информационной безопасности; 80% констатировали финансовые потери от этих нарушений; 44% (223 респондента) смогли и/или захотели оценить потери количественно, общая сумма составила более 455 млн. долларов. Наибольший ущерб нанесли кражи и подлоги (более 170 и 115 млн. долларов соответственно).

Столь же тревожные результаты содержатся в обзоре InformationWeek, опубликованном 12 июля 1999 года. Лишь 22% респондентов заявили об

отсутствии нарушений информационной безопасности. Наряду с распространением вирусов отмечается резкий рост числа внешних атак.

Увеличение числа атак – еще не самая большая неприятность. Хуже то, что постоянно обнаруживаются новые уязвимые места в программном обеспечении и, как следствие, появляются новые виды атак.

Так, в информационном письме Национального центра защиты инфраструктуры США (National Infrastructure Protection Center, NIPC) от 21 июля 1999 года сообщается, что за период с 3 по 16 июля 1999 года выявлено девять проблем с ПО, риск использования которых оценивается как средний или высокий (общее число обнаруженных уязвимых мест равно 17). Среди "пострадавших" операционных платформ – почти все разновидности ОС Unix, Windows, MacOS, так что никто не может чувствовать себя спокойно, поскольку новые ошибки тут же начинают активно использоваться злоумышленниками.

В таких условиях системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание уязвимых мест ведется медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение всех составляющих ИБ – доступности, целостности или конфиденциальности.

Что касается подходов к реализации защитных мероприятий по обеспечению безопасности информационных систем, то сложилась трехэтапная (трехстадийная) разработка таких мер.

Первая стадия – ***выработка требований*** – включает:

- определение состава средств информационной системы;
- анализ уязвимых элементов ИС;
- оценка угроз (выявление проблем, которые могут возникнуть при наличия уязвимых мест);

- анализ риска (прогноз возможных последствий, которые могут вызвать эти проблемы).

Вторая стадия – ***определение способов защиты*** – включает ответы на следующие вопросы:

- Какие угрозы должны быть устранены и в какой мере?
- Какие ресурсы системы должны быть защищаемы и в какой степени?
- С помощью каких средств должна быть реализована защита?
- Какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз?

Третья стадия – ***определение функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты***.

Анализ состояния дел в области информационной безопасности показывает, что в ведущих странах сложились вполне сформировавшиеся концепции и инфраструктура системы защиты информации, основу которой составляют:

- весьма развитый арсенал технических средств защиты, производимых на промышленной основе;
- достаточно четко очерченная система концептуальных взглядов на проблему информационной безопасности;
- наличие значительного практического опыта.

И тем не менее, злоумышленные действия над информацией не только не уменьшаются, а имеют достаточно устойчивую тенденцию к росту.

Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация безопасности информационной системы.

Для защиты АС на основании руководящих документов Гостехкомиссии могут быть сформулированы следующие положения.

1. ИБ АС основывается на положениях требованиях существующих законов, стандартов и нормативно-методических документов.

2. ИБ АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3. ИБ АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

4. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

5. Неотъемлемой частью работ по ИБ является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

6. Защита АС должна предусматривать контроль эффективности средств защиты. Этот контроль может быть периодическим либо инициироваться по мере необходимости пользователем АС или контролирующим органом.

Рассмотренные подходы могут быть реализованы при обеспечении следующих основных принципов:

Принцип комплексности. В распоряжении специалистов по компьютерной безопасности имеется широкий спектр мер, методов и средств защиты компьютерных систем (современные СВТ, операционные системы, инструментальные и прикладные программные средства обладающие теми или иными встроенными элементами защиты). Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Принцип непрерывности защиты. Защита информации - это не разовое мероприятие и даже не конкретная совокупность уже проведенных мероприятий и установленных средств защиты, а непрерывный

целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС (начиная с самых ранних стадий проектирования). Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, позволит создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

Разумная достаточность. Создать абсолютно непреодолимую систему защиты принципиально невозможно; при достаточных времени и средствах можно преодолеть любую защиту. Например, даже средства криптографической защиты не гарантируют абсолютную стойкость, а обеспечивают конфиденциальность информации при использовании для дешифрования современных вычислительных средств в течение приемлемого для защищающейся стороны времени. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов ИС и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Гибкость системы защиты. Часто приходится создавать систему защиты в условиях большой неопределенности. Поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности средства защиты должны обладать определенной гибкостью. Особенно важно это свойство в тех случаях, к средствам защиты необходимо устанавливать на работающую систему, нарушая процесс ее нормального функционирования.

Открытость алгоритмов и механизмов защиты. Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защиту не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления. Но это вовсе не означает, что информация конкретной системе защиты должна быть общедоступна - необходимо обеспечивать защиту от угрозы раскрытия параметров системы.

Принцип простоты применения средств защиты. Механизмы Защиты должны быть интуитивно понятны и просты в использовании, применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных непонятных ему операций (ввод нескольких паролей и имен и т.д.).

В настоящее время можно выделить следущие этапы развития концепций обеспечения безопасности данных, сущность которых приведена в таблице 1.

Таблица 1.

Этапы развития концепций обеспечения безопасности	Характеристика этапа
1 этап 1960-1970 г.г.	Попытки обеспечить безопасность данных чис то формальными механизмами, содержащими, главным образом, технические и программные средства. Сосредоточение программных средств в рамках операционных систвм и систем управления базами данных.
2 этап 1970-1976 г.г.	Дальнейшее развитие формальных механизмов защиты данных. Выделение управляющего компонента защиты данных - ядра безопасности. Развитие неформальных средств защиты. Формирование основ системного подхода к обеспечению безопасности данных.
3 этап 1976-1990 г.г.	Дальнейшее развитие механизмов второго этапа. Формирование взгляда на обеспечение безопасности данных как на непрерывный процесс. Развитие стандартов на средства защиты данных. Усиление тенденции аппаратной реализации средств защиты данных. Формирование вывода о взаимосвязи обеспечения безопасности данных, архитектуры ИВС и технологии ее функционирования. Формирование системного подхода к проблеме обеспечения

	безопасности данных.
4 этап 1990 г. - по настоящее время	Дальнейшее развитие механизмов третьего этапа. Формирование основ теории обеспечения безопасности данных в ИВС. Разработка моделей, методов и алгоритмов управления защитой данных в ИВС.

Глава 2. Методология построения защищенных сетей.

2.1 Задачи управление информационной системой

Управление можно отнести к числу инфраструктурных сервисов, обеспечивающих нормальную работу компонентов и средств безопасности. Сложность современных систем такова, что без правильно организованного управления они постепенно деградируют как в плане эффективности, так и в плане защищенности. Возможен и другой взгляд на ***управление*** – как на интегрирующую оболочку информационных сервисов и сервисов безопасности, обеспечивающую их нормальное, согласованное функционирование под контролем администратора ИС.

Согласно стандарту X.700, управление подразделяется на:

- мониторинг компонентов;
- контроль (то есть выдачу и реализацию управляющих воздействий);
- координацию работы компонентов системы.

Администрирование ИС – действия назначенных лиц (администратора ИС), обеспечивающие поддержание состояния ИС, которые позволяют ей выполнять функциональное предназначение.

Системы управления должны:

- позволять администраторам планировать, организовывать, контролировать и учитывать использование информационных сервисов;
- давать возможность отвечать на изменение требований;
- обеспечивать предсказуемое поведение информационных сервисов;
- обеспечивать защиту информации.

Иными словами, управление должно обладать достаточно богатой функциональностью, быть результативным, гибким и информационно безопасным.

В X.700 выделяется пять функциональных областей управления:

– управление конфигурацией (установка параметров для нормального функционирования, запуск и остановка компонентов, сбор информации о текущем состоянии системы, прием извещений о существенных изменениях в условиях функционирования, изменение конфигурации системы);

– управление отказами (выявление отказов, их изоляция и восстановление работоспособности системы);

– управление учетной информацией (плата за пользование ресурсами);

– управление безопасностью (реализация политики безопасности путем создания, удаления и изменения сервисов и механизмов безопасности, распространения соответствующей информации и реагирования на инциденты);

– управление производительностью (сбор и анализ статистической информации, определение производительности системы в штатных и нештатных условиях, изменение режима работы системы).

Иерархия взаимодействующих менеджеров и агентов может иметь несколько уровней. При этом элементы промежуточных уровней играют двоякую роль: по отношению к вышестоящим элементам они являются агентами, а к нижестоящим – менеджерами. Многоуровневая архитектура менеджер/агент – ключ к распределенному, масштабируемому управлению большими системами.

Обязательным элементом при любом числе архитектурных уровней является управляющая консоль.

С точки зрения изучения возможностей систем управления следует учитывать разделение на следующие аспекты:

– информационный (атрибуты, операции и извещения объектов);

– функциональный (управляющие действия и необходимая для них информация);

– коммуникационный (обмен управляющей информацией);

– организационный (разбиение на области управления).

К числу концептуально важных можно отнести понятие "проактивного", т.е. упреждающего управления, основанного на предсказании поведения системы на основе текущих данных и ранее накопленной информации. (Например, выдача сигнала о возможных проблемах с диском после серии программно-нейтрализуемых ошибок чтения/записи. В более сложном случае определенный характер рабочей нагрузки и действий пользователей может предшествовать резкому замедлению работы системы; адекватным управляющим воздействием могло бы стать понижение приоритетов некоторых заданий и извещение администратора о приближении кризиса).

2.2 Протоколирование и аудит

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

Под ***протоколированием*** понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически. ***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, по крайней мере, 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. Выявление и анализ проблем могут помочь улучшить такой параметр безопасности, как доступность. Обнаружив узкие места, можно попытаться переконфигурировать или перенастроить систему, снова измерить производительность и т.д.

Непросто осуществить организацию согласованного протоколирования и аудита в распределенной разнородной системе. Во-первых, некоторые компоненты, важные для безопасности (например, маршрутизаторы), могут не обладать своими ресурсами протоколирования; в таком случае их нужно экранировать другими сервисами, которые возьмут протоколирование на себя. Во-вторых, необходимо увязывать между собой события в разных сервисах.

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. 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. (Пример сигнатуры – "зафиксированы три последовательные неудачные попытки входа в систему с одного терминала", пример ассоциированной реакции – блокирование терминала до прояснения ситуации).

Действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности, называться ***злоупотреблением полномочиями*** (пример – неэтичное поведение суперпользователя, просматривающего файлы других пользователей).

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 ИС. На границе контролируемой зоны можно обнаружить подозрительную активность в точках подключения к внешним сетям. В корпоративной сети активный аудит в состоянии обнаружить и пресечь подозрительную активность внешних и внутренних пользователей, выявить проблемы в работе сервисов, вызванные как нарушениями безопасности, так и

аппаратно-программными ошибками. Активный аудит может обеспечить защиту от атак на доступность.

Функциональные компоненты и архитектура

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 извлечения регистрационной информации (сенсоры).

Обычно различают сетевые и хостовые сенсоры, имея в виду под первыми выделенные компьютеры, сетевые карты которых установлены в режим прослушивания, а под вторыми – программы, читающие регистрационные журналы операционной системы. С развитием коммутационных технологий это различие постепенно стирается, так как сетевые сенсоры приходится устанавливать в активном сетевом оборудовании и они становятся частью сетевой ОС:

- компоненты просмотра регистрационной информации;
- компоненты анализа информации, поступившей от сенсоров;
- компоненты хранения информации, участвующей в анализе;
- компоненты принятия решений и реагирования ("решатели");
- компоненты хранения информации о контролируемых объектах;
- компоненты, играющие роль организующей оболочки для менеджеров активного аудита, называемые мониторами и объединяющие анализаторы;
- компоненты интерфейса с администратором безопасности.

Средства активного аудита строятся в архитектуре менеджер/агент. Основными агентскими компонентами являются сенсоры. Анализ, принятие решений – функции менеджеров. Очевидно, между менеджерами и агентами должны быть сформированы доверенные каналы.

Наибольшее распространение для установления подлинности в настоящее время получили методы паролирования.

Методы паролирования требуют, чтобы пользователь ввел строку символов (пароль) для сравнения с эталонным паролем, хранящимся в памяти системы. Если пароль соответствует эталонному, то пользователь может работать с системой.

При рассмотрении различных методов паролирования будем пользоваться следующими обозначениями: С - сообщение системы; П - сообщение, вводимое пользователем; ОК - сообщение системы о правильном установлении подлинности.

Метод простого пароля состоит во вводе пользователем одного пароля с клавиатуры.

Пример 1 (Паролем является слово "ПАРОЛЬ").

С: Введите пароль

П: ПАРОЛЬ

С: ОК

Метод выборки символов состоит в запросе системой определенных символов пароля, выбираемых случайным образом.

Пример 2. (Паролем является слово "ПАРОЛЬ").

С: Введите пароль: 2, 5

П: АЛ

С: ОК

Метод выборки символов не позволяет нарушителю определить значение пароля по однократному наблюдению вводимых пользователем символов.

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***.

Метод паролей однократного использования предполагает наличие списка из N паролей, хранящегося в системе. При каждом обращении к системе пользователь вводит очередной пароль, который после окончания работы вычеркивается системой из списка.

Наиболее известным программным генератором одноразовых паролей является система **S/KEY** компании Bellcore, имеющая статус Internet-стандарта (RFC 1938). Идея этой системы состоит в следующем. Пусть имеется **односторонняя функция** f (то есть функция, вычислить обратную которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и **серверу аутентификации**. Пусть, далее, имеется **секретный ключ** K, известный только пользователю.

На этапе начального администрирования пользователя функция f применяется к ключу K n раз, после чего результат сохраняется на сервере. После этого процедура проверки подлинности пользователя выглядит следующим образом:

- сервер присылает на пользовательскую систему число (n-1);
- пользователь применяет функцию f к секретному ключу K (n-1) раз и отправляет результат по сети на сервер аутентификации;
- сервер применяет функцию f к полученному от пользователя значению и сравнивает результат с ранее сохраненной величиной. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик (n).

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой интервал времени (например, каждые 60 секунд),

для чего используются программы или специальные интеллектуальные карты.

Метод групп паролей основывается на том, что система для каждого пользователя может потребовать пароли из двух групп.

Первая группа включает пароли, которые являются ответами на общие для всех пользователей вопросы, например, имя, адрес, номер телефона и т.п. Вторая группа включает пароли - ответы на вопросы, которые устанавливаются администратором системы при регистрации пользователя для работы с системой. Эти вопросы сформулированы персонально для каждого пользователя, например, любимый цвет, девичья фамилия матери и т.п. При каждом обращении пользователя система случайно выбирает по нескольку вопросов из каждой группы. Недостатком рассмотренного метода является то, что системе потребуется значительный объем памяти для хранения вопросов и ответов для большого числа пользователей.

Метод функционального преобразования предполагает, что пользователю при регистрации для работы в системе сообщается некоторое преобразование, которое он может выполнить в уме. Паролем в этом случае является результат такого преобразования.

Пример 3. (Преобразование y=x1+2*x2).

С: Введите пароль: 4, 6

П: 16

С: ОК

При работе с паролями должны соблюдаться следующие правила:

- пароли должны храниться в памяти только в зашифрованном виде;
- символы пароля при вводе их пользователем не должны появляться в явном виде;
- пароли должны периодически меняться;
- пароли не должны быть простыми.

Для проверки сложности паролей обычно используют специальные контроллеры паролей.

В настоящее время существует контроллер паролей, который позволяет проверить уязвимость паролей. Контроллер осуществляет попытки взлома пароля по следующей методике.

1. Проверка использования в качестве пароля входного имени пользователя, его инициалов и их комбинаций. Например, для пользователя Daniel V. Klein (автор контроллера) контроллер будет пробовать пароли DVK, DVKDVK, DKLEIN, LEINK, DVKLEIN, DANIELK, DVKKVD, DANIEL-KLEIN и т.д.

2. Проверка использования в качестве пароля слов из различных словарей (60000 слов):

- мужские и женские имена (16000 имен);
- названия стран и городов;
- имена персонажей мультфильмов, кинофильмов, научно - фантастических произведений и т.п.;
- спортивные термины (названия команд, имена спортсменов, спортивный жаргон и т.п.);
- числа (цифрами и прописью, например, 2000, TWELVE);
- строки букв и цифр (например, AA, AAA, AAAA и т.д.);
- библейские имена и названия;
- биологические термины;
- жаргонные слова и ругательства;
- последовательности символов в порядке их расположения на клавиатуре (например, QWERTY, ASDF, ZXCVBN и т.д.);
- имена компьютеров (из файла /etc/hostc в ОС Unix);
- персонажи и места действия из произведений Шекспира;
- часто употребляемые иностранные слова;
- названия астероидов.

3. Проверка различных перестановок слов из п.2, включая:

- замену первой буквы на прописную;

- замену всех букв на прописные;

- инверсию всего слова;

- замену буквы О на цифру 0 и наоборот (цифру 1 на букву 1 и т.д.);

- превращение слов во множественное число.

Всего по п.3 контроллер осуществляет проверку на совпадение приблизительно с 1 миллионом слов.

4. Проверка различных перестановок слов из п.2, не рассмотренных в п.3:

-замена одной строчной буквы на прописную (например, michel-miChel и т.п.- около 400000 слов);

- замена двух строчных букв на прописные (около 1500000 слов);

- замена трех строчных букв на прописные и т.д.

5. Для иностранных пользователей проверка слов на языке пользователя.

6. Проверка пар слов.

Проведенные эксперименты показали, что данный контроллер позволил определить 10% паролей из пяти символов, 35% паролей из шести символов, 25% паролей из семи символов и 23% паролей из восьми символов. Это вызвано тем, что большинство пользователей используют простые пароли. Данным обстоятельством воспользовался Р.Моррис - автор "сетевого червя", заразившего сеть Интернет в 1988 году. Модуль захвата вируса Морриса осуществлял опробование в качестве паролей учетные имена пользователей, учетные имена пользователей в обратном порядке, а также пароли из шаблона, состоящего из 432 общеизвестных слов. В отдельных случаях Моррис сумел получить до 10% паролей, в том числе и ряд системных паролей.

Вместе с тем паролирование является наименее защищенным средством аутентификации. Ввод пароля можно подсмотреть. Иногда для подглядывания используются даже оптические приборы. 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.

Следующие меры позволяют повысить надежность парольной защиты:

- ***наложение технических ограничений*** (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- ***управление сроком действия паролей***, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");
- обучение пользователей;
- использование программных ***генераторов паролей*** (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Если для аутентификации должны использоваться электронные подписи, то требуется использование сертификатов. Сертификаты обычно состоят из какой-то информации и электронной подписи информационной части сертификата, выданной доверенным лицом. Пользователи могут получить сертификаты различных уровней.

2.3 Контроль за импортом програм

Данные на компьютерах редко бывают статичными. Принимаются новые электронные письма. Новые программы загружаются с дискет, CD-ROMов, или с серверов сети. Интерактивные веб-программы загружают выполняемые файлы, которые выполняются на компьютере. Любое изменение несет в себе

риск заражения вирусами, разрушения конфигурации компьютера, или нарушения лицензий на использование программ. Организациям нужно защищаться с помощью различных механизмов в зависимости от уязвимости к этим рискам.

Контроль за импортом программ позволяет решить следующие задачи:

– защита от вирусов и «троянских коней», их обнаружение и удаление;

– контроль за интерактивными программами(Java, Active X);

– контроль за соблюдением лицензий на программы.

Каждая задача может быть классифицирована по следующим критериям:

– контроль – кто является инициатором процесса, и как можно определить, что была импортирована программа;

– тип угрозы – выполняемая программа, макрос, апплет, нарушение лицензионного соглашения;

– контрмеры – проверка на вирусы, отключение сервиса, изменение прав по доступу, аудирование, удаление.

При импорте программ на компьютере и их запуске на нем имеется риск, что эти программы обладают дополнительной функциональностью или их реальные функции отличаются от заявленных. Импорт может происходить в форме непосредственного действия пользователя или являться побочным эффектом других действий и не быть заметен. Примерами явного импорта являются: передача файлов - использование FTP для переноса файла на PC, чтение электронной почты, загрузка программ с дискеты или по сети и др. Примерами скрытого импорта является чтение веб-страницы, загружающей Java-апплет на ваш компьютер или открытие файла, зараженного макро-вирусом.

2.4 Зашита от вирусов

Вначале самым распространенным способом заражения вирусами были дискеты, так как именно с их помощью переносились программы между компьютерами. После появления BBS вирусы стали распространяться через модем. Интернет привел к появлению еще одного канала распространения вирусов, с помощью которого они часто обходят традиционные методы борьбы с ними.

Для организаций, которые разрешают загружать программы из глобальных сетей (которые могут быть приложениями к электронным письмам), проверка программ на вирусы на МЭ может оказаться хорошим.

Политика безопасности для борьбы с вирусами имеет три части:

– предотвращение – правила, позволяющие предотвратить заражение;

– обнаружение – как определить, что данный выполняемый файл, загрузочная запись, или файл данных содержит вирус;

– удаление – удаление вируса из зараженной компьютерной системы (переинсталляция ОС, удаление файлов, удаление вируса из зараженного файла.

Вероятность заражения вирусами пропорциональна частоте появления новых файлов или приложений на компьютере, а также изменениям в конфигурации для работы в Интернете, чтения электронной почты и загрузка файлов из внешних источников. Чем больше значение компьютера или данных, находящихся в нем, тем больше надо позаботиться о мерах безопасности против вирусов. Политика предотвращения может обращать особое внимание на ограничения на загрузку потенциально зараженных программ и файлов. В ней также может быть указано, что в среде с высоким риском проверка на вирусы особенно тщательно должна производиться для новых файлов.

2.4.1 Контроль интерактивных программ

Программная среда в результате появления Интернета превратилась в среду интерактивных программ, примерами которой являются Java и Active X. В этой среде пользователь взаимодействует с сервером с помощью сети. Сервер загружает приложение (апплет) на пользовательский компьютер, который затем его выполняет. При использовании такой стратегии имеет место несколько рисков. Прежде всего нужно верит, что то, что загружается, делает именно то, что должно делать.

Ранее утверждалось, что при использовании таких языков как Java невозможно занести вирус из-за ограничений, встроенных в язык для управления доступом к файловой системе и для управления выполнением программы. Сейчас эти заявления достаточно эффективно опровергнуты. Из-за значительного риска существует несколько уровней гарантий безопасности, которые должен получить пользователь перед использованием этой технологии:

– сервер, с которого загружаются апплеты, должен быть доверенным;

– апплет должен выполняться в среде с ограничениями на обращения к файлам, реализующей только те функции, которые не влияют на безопасность;

– апплет должен быть проверен на безопасность перед выполнением;

– скрипты интерпретируются, а не являются предварительно скомпилированными.

–

2.4.2 Лицензирование программ

Интернет позволил многим организациям использовать новые пути распространения программ. Большое число компаний позволяют

пользователям загружать тестовые версии их продуктов, иногда демо-версии, или версии, которые работают ограниченное время. Тем не менее, много компаний применяют подход shareware, при котором можно загружать полнофункциональные версии программ для тестирования, а пользователь должен зарегистрироваться и заплатить, если он будет использовать программу в коммерческих целях.

Когда пользователи не регистрируются или делают это неправильно с программами, загруженными через Интернет, организация может оказаться нарушителем правил лицензирования программ. Это может привести к судебным искам, или потере репутации при обнаружении таких фактов.

Низкий риск – следует соблюдать правила лицензий производителей программ для всех коммерческих программ, загруженных по Интернету. Тестовые версии программ должны быть удалены по истечении периода тестирования, или организацией должна быть приобретена легальная версия программы.

Средний-высокий риск – коммерческие программы запрещается загружать без разрешения сисадмина. Программы, используемые на компьютерах организации, установливаются только системными администраторами в соответствии с правилами лицензий. Сотрудники отдела автоматизации должны периодически инспектировать компьютеры на предмет соблюдения правил лицензий и отсутствия неразрешенных программ.

Глава 3. Тенденция развития и применения методов и средств защиты информации в компьютерных системах

3.1 Основные методы зашиты в сетях.

Цель мероприятий в области **информационной безопасности** – защитить **интересы субъектов информационных отношений**. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов:

- **доступность**;
- **целостность**;
- **конфиденциальность**.

Первый шаг при построении системы **ИБ** организации – ранжирование и детализация этих аспектов.

Важность проблематики ИБ объясняется двумя основными причинами:

- ценностью накопленных информационных ресурсов;
- критической зависимостью от информационных технологий.

Разрушение важной информации, кража конфиденциальных данных, перерыв в работе вследствие отказа – все это выливается в крупные материальные потери, наносит **ущерб** репутации организации. Проблемы с системами управления или медицинскими системами угрожают здоровью и жизни людей.

Современные информационные системы сложны и, значит, опасны уже сами по себе, даже без учета активности злоумышленников. Постоянно обнаруживаются новые **уязвимые места** в программном обеспечении. Приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Меняются принципы построения корпоративных ИС. Используются многочисленные внешние информационные сервисы; предоставляются вовне

собственные; получило широкое распространение явление, обозначаемое исконно русским словом "аутсорсинг", когда часть функций корпоративной ИС передается внешним организациям. Развивается программирование с **активными агентами**.

Подтверждением **сложности** проблематики ИБ является параллельный (и довольно быстрый) **рост затрат** на защитные мероприятия и количества **нарушений** ИБ в сочетании с ростом среднего ущерба от каждого нарушения. (Последнее обстоятельство - еще один довод в пользу важности ИБ.)

Успех в области информационной безопасности может принести только комплексный подход, сочетающий меры четырех **уровней**:

- **законодательного**;
- **административного**;
- **процедурного**;
- **программно-технического**.

Проблема ИБ – не только и не столько техническая; без законодательной базы, без постоянного внимания руководства организации и выделения необходимых ресурсов, без мер управления персоналом и физической защиты решить ее невозможно. Комплексность также усложняет проблематику ИБ; требуется взаимодействие специалистов из разных областей.

В качестве основного инструмента борьбы со сложностью предлагается **объектно-ориентированный подход**. **Инкапсуляция**, **наследование**, **полиморфизм**, выделение **граней** объектов, варьирование **уровня детализации** – все это универсальные понятия, знание которых необходимо всем специалистам по информационной безопасности.

Законодательный, административный и процедурный уровни

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Необходимо всячески подчеркивать

важность проблемы ИБ; сконцентрировать ресурсы на важнейших направлениях исследований; скоординировать образовательную деятельность; создать и поддерживать негативное отношение к нарушителям ИБ – все это функции законодательного уровня.

На законодательном уровне особого внимания заслуживают **правовые акты** и **стандарты**.

Российские правовые акты в большинстве своем имеют ограничительную направленность. Но то, что для Уголовного или Гражданского кодекса естественно, по отношению к Закону об информации, информатизации и защите информации является принципиальным недостатком. Сами по себе **лицензирование** и **сертификация** не обеспечивают безопасности. К тому же в законах не предусмотрена ответственность государственных органов за нарушения ИБ. Реальность такова, что в России в деле обеспечения ИБ на помощь государства рассчитывать не приходится.

На этом фоне поучительным является знакомство с законодательством США в области ИБ, которое гораздо обширнее и многограннее российского.

Среди стандартов выделяются **"Оранжевая книга"**, рекомендации **X.800** и "Критерии оценки безопасности информационных технологий".

"Оранжевая книга" заложила понятийный базис; в ней определяются важнейшие **сервисы безопасности** и предлагается метод **классификации** информационных систем по требованиям безопасности.

Рекомендации X.800 весьма глубоко трактуют вопросы защиты **сетевых конфигураций** и предлагают развитый набор сервисов и **механизмов безопасности**.

Международный стандарт ISO 15408, известный как **"Общие критерии"**, реализует более современный подход, в нем зафиксирован чрезвычайно широкий спектр сервисов безопасности (представленных как **функциональные требования**). Его принятие в качестве национального стандарта важно не только из абстрактных соображений интеграции в

мировое сообщество; оно, как можно надеяться, облегчит жизнь владельцам информационных систем, существенно расширив спектр доступных сертифицированных решений.

Главная задача мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является **политика безопасности**, отражающая подход организации к защите своих информационных активов.

Разработка политики и **программы безопасности** начинается с **анализа рисков**, первым этапом которого, в свою очередь, является ознакомление с наиболее распространенными **угрозами**.

Главные угрозы – внутренняя сложность ИС, непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

На втором месте по размеру ущерба стоят кражи и подлоги.

Реальную опасность представляют пожары и другие аварии поддерживающей инфраструктуры.

В общем числе нарушений растет доля внешних атак, но основной ущерб по-прежнему наносят "свои".

Для подавляющего большинства организаций достаточно общего знакомства с рисками; ориентация на типовые, апробированные решения позволит обеспечить **базовый уровень безопасности** при минимальных интеллектуальных и разумных материальных затратах.

Существенную помощь в разработке политики безопасности может оказать британский стандарт BS 7799:1995, предлагающий типовой каркас.

Разработка программы и политики безопасности может служить примером использования понятия уровня детализации. Они должны подразделяться на несколько уровней, трактующих вопросы разной степени

специфичности. Важным элементом программы является разработка и поддержание в актуальном состоянии карты ИС.

Необходимым условием для построения надежной, экономичной защиты является рассмотрение **жизненного цикла** ИС и синхронизация с ним мер безопасности. Выделяют следующие этапы жизненного цикла:

- инициация;
- закупка;
- установка;
- эксплуатация;
- выведение из эксплуатации.

Безопасность невозможно добавить к системе; ее нужно закладывать с самого начала и поддерживать до конца.

Меры процедурного уровня ориентированы на людей (а не на технические средства) и подразделяются на следующие виды:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

На этом уровне применимы важные принципы безопасности:

- непрерывность защиты в пространстве и времени;
- разделение обязанностей;
- минимизация привилегий.

Здесь также применимы объектный подход и понятие жизненного цикла. Первый позволяет разделить контролируемые сущности (территорию, аппаратуру и т.д.) на относительно независимые подобъекты, рассматривая их с разной степенью детализации и контролируя связи между ними.

Понятие жизненного цикла полезно применять не только к информационным системам, но и к сотрудникам. На этапе инициации

должно быть разработано описание должности с требованиями к квалификации и выделяемыми компьютерными привилегиями; на этапе установки необходимо провести обучение, в том числе по вопросам безопасности; на этапе выведения из эксплуатации следует действовать аккуратно, не допуская нанесения ущерба обиженными сотрудниками.

Информационная безопасность во многом зависит от аккуратного ведения текущей работы, которая включает:

- поддержку пользователей;
- поддержку программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Элементом повседневной деятельности является отслеживание информации в области ИБ; как минимум, администратор безопасности должен подписаться на список рассылки по новым пробелам в защите (и своевременно знакомиться с поступающими сообщениями).

Нужно, однако, заранее готовиться к событиям неординарным, то есть к нарушениям ИБ. Заранее продуманная реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

Выявление нарушителя – процесс сложный, но первый и третий пункты можно и нужно тщательно продумать и отработать.

В случае серьезных аварий необходимо проведение восстановительных работ. Процесс планирования таких работ можно разделить на следующие этапы:

- выявление критически важных функций организации, установление приоритетов;
- идентификация ресурсов, необходимых для выполнения критически важных функций;
- определение перечня возможных аварий;
- разработка стратегии восстановительных работ;
- подготовка к реализации выбранной стратегии;
- проверка стратегии.

Программно-технические меры

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей – оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности.

На этом рубеже становятся очевидными не только позитивные, но и негативные последствия быстрого прогресса информационных технологий. Во-первых, дополнительные возможности появляются не только у специалистов по ИБ, но и у злоумышленников. Во-вторых, информационные системы все время модернизируются, перестраиваются, к ним добавляются недостаточно проверенные компоненты (в первую очередь программные), что затрудняет соблюдение режима безопасности.

Сложность современных корпоративных ИС, многочисленность и разнообразие угроз их безопасности можно наглядно представить, ознакомившись с информационной системой Верховного суда Российской Федерации.

Меры безопасности целесообразно разделить на следующие виды:

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

В продуманной **архитектуре безопасности** все они должны присутствовать.

С практической точки зрения важными также 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.

Центральным для программно-технического уровня является понятие сервиса безопасности. В число таких сервисов входят:

- **идентификация** и **аутентификация**;
- **управление доступом**;
- **протоколирование** и **аудит**;
- **шифрование**;
- **контроль целостности**;
- **экранирование**;
- **анализ защищенности**;
- обеспечение **отказоустойчивости**;
- обеспечение **безопасного восстановления**;
- **туннелирование**;

- **управление**.

Эти сервисы должны функционировать в открытой сетевой среде с разнородными компонентами, то есть быть устойчивыми к соответствующим угрозам, а их применение должно быть удобным для пользователей и администраторов. Например, современные средства идентификации/аутентификации должны быть устойчивыми к пассивному и активному прослушиванию сети и поддерживать концепцию единого входа в сеть.

Выделим важнейшие моменты для каждого из перечисленных сервисов безопасности:

1. Предпочтительными являются **криптографические методы** аутентификации, реализуемые программным или аппаратно-программным способом. Парольная защита стала анахронизмом, биометрические методы нуждаются в дальнейшей проверке в сетевой среде.

2. В условиях, когда понятие доверенного программного обеспечения уходит в прошлое, становится анахронизмом и самая распространенная – произвольная (дискреционная) – модель управления доступом. В ее терминах невозможно даже объяснить, что такое "троянская" программа. В идеале при **разграничении доступа** должна учитываться семантика операций, но пока для этого есть только теоретическая база. Еще один важный момент – простота администрирования в условиях большого числа пользователей и ресурсов и непрерывных изменений конфигурации. Здесь может помочь ролевое управление.

Протоколирование и аудит должны быть всепроникающими и многоуровневыми, с фильтрацией данных при переходе на более высокий уровень. Это необходимое условие управляемости. Желательно применение средств **активного аудита**, однако нужно осознавать ограниченность их возможностей и рассматривать эти средства как один из рубежей эшелонированной обороны, причем не самый надежный. Следует

конфигурировать их таким образом, чтобы минимизировать число ложных тревог и не совершать опасных действий при автоматическом реагировании.

Все, что связано к криптографией, сложно не столько с технической, сколько с юридической точки зрения; для шифрования это верно вдвойне. Данный сервис является инфраструктурным, его реализации должны присутствовать на всех аппаратно-программных платформах и удовлетворять жестким требованиям не только к безопасности, но и к производительности. Пока же единственным доступным выходом является применение свободно распространяемого ПО.

Надежный контроль целостности также базируется на криптографических методах с аналогичными проблемами и методами их решения. Возможно, принятие Закона об **электронной цифровой подписи** изменит ситуацию к лучшему, будет расширен спектр реализаций. К счастью, к статической целостности есть и некриптографические подходы, основанные на использовании запоминающих устройств, данные на которых доступны только для чтения. Если в системе разделить статическую и динамическую составляющие и поместить первую в ПЗУ или на компакт-диск, можно в корне пресечь угрозы целостности. Разумно, например, записывать регистрационную информацию на устройства с однократной записью; тогда злоумышленник не сможет "замести следы".

Экранирование – идейно очень богатый сервис безопасности. Его реализации – это не только межсетевые экраны, но и ограничивающие интерфейсы, и виртуальные локальные сети. Экран инкапсулирует защищаемый объект и контролирует его внешнее представление. Современные межсетевые экраны достигли очень высокого уровня защищенности, удобства использования и администрирования; в сетевой среде они являются первым и весьма мощным рубежом обороны. Целесообразно применение всех видов МЭ – от персонального до внешнего

корпоративного, а контролю подлежат действия как внешних, так и внутренних пользователей.

Анализ защищенности – это инструмент поддержки безопасности жизненного цикла. С активным аудитом его роднит эвристичность, необходимость практически непрерывного обновления базы знаний и роль не самого надежного, но необходимого защитного рубежа, на котором можно расположить свободно распространяемый продукт.

Обеспечение отказоустойчивости и безопасного восстановления – аспекты высокой доступности. При их реализации на первый план выходят архитектурные вопросы, в первую очередь – внесение в конфигурацию (как аппаратную, так и программную) определенной избыточности, с учетом возможных угроз и соответствующих зон поражения. Безопасное восстановление – действительно последний рубеж, требующий особого внимания, тщательности при проектировании, реализации и сопровождении.

Туннелирование – скромный, но необходимый элемент в списке сервисов безопасности. Он важен не столько сам по себе, сколько в комбинации с шифрованием и экранированием для реализации виртуальных частных сетей.

Управление – это инфраструктурный сервис. Безопасная система должна быть управляемой. Всегда должна быть возможность узнать, что на самом деле происходит в ИС (а в идеале – и получить прогноз развития ситуации). Возможно, наиболее практичным решением для большинства организаций является использование какого-либо свободно распространяемого каркаса с постепенным "навешиванием" на него собственных функций.

3.2 Криптографическая зашита информации в сетях.

История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была своеобразной

криптографической системой, так как в древних обществах ею владели только избранные.

Развитию тайнописи способствовали войны. Письменные приказы и донесения обязательно шифровались, чтобы пленение курьеров не позволило противнику получить важную информацию. Например, римский император Цезарь пользовался в своей военной и личной переписке шифром, сущность которого состояла в замене каждой буквы латинского языка на следующую букву алфавита. Знаменитая фраза: «VENI, VIDI, VICI» («Пришел, увидел, победил»), которой Цезарь, известил одного из своих друзей в Риме о быстро одержанной им победе, в зашифрованном виде будет выглядеть так: "XFOJ, XJEJ, XJDJ".

Практически одновременно с криптографией стал развиваться и криптоанализ – наука о раскрытии шифров (ключей) по шифртексту.

История криптографии условно можно разделить на 4 этапа: наивная криптография; формальная криптография; научная криптография; компьютерная криптография.

Для ***наивной криптографии*** (до нач. XVI века) характерно использование любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов. На начальном этапе для защиты информации использовались методы *кодирования* и *стеганографии,* которые родственны, но не тождественны криптографии.

Большинство из используемых шифров сводились к *перестановке* или *моноалфавитной подстановке.* Одним из первых зафиксированных примеров является шифр Цезаря, состоящий в замене каждой буквы исходного текста на другую, отстоящую от нее в алфавите на определенное число позиций. Другой шифр, полибианский квадрат, авторство которого приписывается греческому писателю Полибию, является общей моноалфавитной подстановкой, которая проводится с помощью случайно заполненной алфавитом квадратной таблицей (для греческого алфавита

размер составляет 5x5). Каждая буква исходного текста заменяется на букву, стоящую в квадрате снизу от нее.

Этап ***формальной криптографии*** (кон. XV века - нач. XX века) связан с появлением формализованных и относительно стойких к ручному криптоанализу шифров. В европейских странах это произошло в эпоху Возрождения, когда развитие науки и торговли вызвало спрос на надежные способы защиты информации. Важная роль на этом этапе принадлежит Леону Батисте Альберти, итальянскому архитектору, который одним из первых предложил *многоалфавитную подстановку.* Данный шифр, получивший имя дипломата Блеза Вижинера, состоял в последовательном «сложении» букв исходного текста с ключом (процедуру можно облегчить с помощью специальной таблицы). Его работа «Трактат о шифре» (1466) считается первой научной работой по криптологии.

Одной из первых печатных работ, обобщающей известные на тот момент алгоритмы шифрования является труд «Полиграфия» (1508 г.) немецкого аббата Иоганна Трисемуса. Ему принадлежат два небольших, но важных открытия: способ заполнения полибианского квадрата и шифрование пар букв (биграмм).

Простым, но стойким способом многоалфавитной замены (подстановки биграмм) является шифр Плейфера, который был открыт в начале XIX века Чарльзом Уитстоном. Ему принадлежит и важное усовершенствование - шифрование «двойным квадратом». Шифры Плейфера и Уитстона использовались до первой мировой войны, т.к. с трудом поддавались ручному криптоанализу.

В XIX веке голландец Керкхофф сформулировал главное требование к криптосистемам, которое остается актуальным и поныне: ***секретность шифров должна быть основана на секретности ключа, но не алгоритма***.

Последним словом в донаучной криптографии, которое обеспечили более высокую криптостойкосить, а также позволило автоматизировать (в смысле механизировать) процесс шифрования стали ***роторные криптосистемы***.

Одной из первых подобных систем стала изобретенная в 1790 году Томасом Джефферсоном, будущим президентом США механическая машина. Многоалфавитная подстановка с помощью роторной машины реализуется вариацией взаимного положения вращающихся роторов, каждый из которых осуществляет «прошитую» в нем подстановку.

Практическое распространение роторные машины получили в начале XX века. Одной из первых практически используемых машин, стала немецкая Enigma, разработанная в 1917 году Эдвардом Хеберном и усовершенствованная Артуром Кирхом. Роторные машины активно использовались во время второй мировой войны. Помимо немецкой машины Enigma использовались также устройства Sigaba (США), Typex (Великобритания), Red, Orange и Purple (Япония). Роторные системы – вершина формальной криптографии, так как относительно просто реализовывали очень стойкие шифры. Успешные криптоатаки на роторные системы стали возможны только с появлением ЭВМ в начале 40-х годов.

Главная отличительная черта ***научной криптографии*** (30-е - 60-е годы XX века) - появление криптосистем со строгим математическим обоснованием криптостойкости. К началу 30-х годов окончательно сформировались разделы математики, являющиеся научной основой криптологии: теория вероятностей и математическая статистика, общая алгебра, теория чисел, начали активно развиваться теория алгоритмов, теория информации, кибернетика. Своеобразным водоразделом стала работа Клода Шеннона «Теория связи в секретных системах» (1949), которая подвела научную базу под криптографию и криптоанализ. С этого времени стали говорить о ***КРИПТОЛОГИИ*** (от греческого kryptos – тайный и logos – учение) – науке о преобразовании информации для обеспечения ее

секретности. Этап развития криптографии и криптоанализа до 1949 года стали называть донаучной криптологией. Шеннон ввел понятия «рассеивание» и «перемешивание», обосновал возможность создания сколь угодно стойких криптосистем.

В 60-х годах ведущие криптографические школы подошли к созданию *блочных шифров,* еще более стойких по сравнению с роторными криптосистемами, однако допускающие практическую реализацию только в виде цифровых электронных устройств.

Компьютерная криптография (с 70-х годов XX века) обязана своим появлением вычислительным средствам с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем «ручные» и «механические» шифры.

Первым классом криптосистем, практическое применение которых стало возможно с появлением мощных и компактных вычислительных средств, стали блочные шифры. В 70-е годы был разработан *американский стандарт шифрования DES* (принят в 1978 году). Один из его авторов, Хорст Фейстел (сотрудник IBM), описал модель блочных шифров, на основе которой были построены другие, более стойкие симметричные криптосистемы, в том числе *отечественный стандарт шифрования ГОСТ 28147-89.*

С появлением DES обогатился и криптоанализ, для атак на американский алгоритм был создано несколько новых видов криптоанализа (линейный, дифференциальный и т.д.), практическая реализация которых опять же была возможна только с появлением мощных вычислительных систем.

В середине 70-х годов произошел настоящий прорыв в современной криптографии - *появление асимметричных криптосистем,* которые не требовали передачи секретного ключа между сторонами. Здесь отправной точкой принято считать работу, опубликованную Уитфилдом Диффи и Мартином Хеллманом в 1976 году под названием «Новые направления в

современной криптографии». В ней впервые сформулированы принципы обмена шифрованной информацией без обмена секретным ключом. Независимо к идее асимметричных криптосистем подошел Ральф Меркли. Несколькими годами позже Рон Ривест, Ади Шамир и Леонард Адлеман открыли систему RSA, первую практическую асимметричную криптосистему, стойкость которой была основана на проблеме *факторизации* больших простых чисел. Асимметричная криптография открыла сразу несколько новых прикладных направлений, в частности, системы *электронной цифровой подписи (ЭЦП)* и *электронных денег.*

В 80-90-е годы появились совершенно новые направления криптографии: вероятностное шифрование, квантовая криптография и другие. Актуальной остается и задача совершенствования симметричных криптосистем. В 80-90-х годах были разработаны нефейстеловские шифры (SAFER, RC6 и др.), а в 2000 году после открытого международного конкурса был принят новый национальный стандарт шифрования США – AES.

Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности. Например, для портативных компьютеров, физически защитить которые крайне трудно, только криптография позволяет гарантировать конфиденциальность информации даже в случае кражи.

Криптографическая защита информации необходимо и тогда, когда данные никуда не перемещаются, т.к. события могут развиваться не только в пространстве, но и во времени.

Подробнее об истории криптографии можно прочитать в книге [В. Жельников. Криптография от папируса до компьютера –М.: Dore Print, 1999. 214 с.].

Наукой, изучающей математические методы защиты информации путем ее преобразования, является ***криптология***. Криптология разделяется на два направления – *криптографию* и *криптоанализ.*

Криптография изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность.

Под ***конфиденциальностью*** понимают невозможность получения информации из преобразованного массива без знания дополнительной информации (ключа).

Аутентичность информации состоит в *подлинности авторства* и *целостности.*

Криптоанализ объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.

Существует ряд смежных, но не входящих в криптологию отраслей знания. Так обеспечением *скрытности* информации в информационных массивах занимается ***стеганография***. Обеспечение целостности информации в условиях случайного воздействия находится в ведении ***теории помехоустойчивого кодирования***. Наконец, смежной областью по отношению к криптологии являются ***математические методы сжатия информации***.

Современная криптография включает в себя четыре крупных раздела: *симметричные* криптосистемы; *асимметричные* криптосистемы (с открытым ключом); *системы электронной подписи*; *управление ключами*.

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи, установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

В качестве информации, подлежащей шифрованию и расшифрованию, а также электронной подписи будут рассматриваться *тексты (сообщения),* построенные на некотором *алфавите.*

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст (сообщение) – упорядоченный набор из элементов алфавита. Примерами алфавитов, используемых в современных ИС, являются:

- алфавит Z_{33} – 32 буквы русского алфавита (исключая "ё") и пробел;
- алфавит Z_{256} – символы, входящие в стандартные коды ASCII и КОИ-8;
- двоичный алфавит – $Z_2 = \{0,1\}$;
- восьмеричный или шестнадцатеричный алфавит.

Коды и шифры использовались задолго до появления ЭВМ. С точки зрения теории не существует четкого различия между кодами и шифрами. Однако на практике различие между ними является достаточно четким. ***Коды*** оперируют *лингвистическими элементами*, разделяя шифруемый текст на смысловые элементы (слова и слоги), а в ***шифре*** – всегда два элемента: *алгоритм и ключ*.

Алгоритм позволяет использовать сравнительно короткий ключ для шифрования сколь угодно большого текста.

Определим ряд терминов, используемых в криптологии.

Под ***шифром*** понимается совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования.

Шифр - это совокупность инъективных отображений множества открытых текстов во множество шифрованных текстов, проиндексированная элементами из множества ключей: $\{F_k : X \to S,\ k \in K\}$.

Криптографическая система, или ***шифр*** представляет собой семейство T обратимых преобразований открытого текста в шифрованный. Членам

этого семейства взаимно однозначно сопоставляется число *k,* называемое *ключом.* Преобразование T_k определяется соответствующим алгоритмом и значением ключа *k.*

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма. Секретность ключа должна обеспечивать невозможность восстановление исходного текста по шифрованному.

Пространство ключей К – это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита. Следует отличать понятия ключ и пароль. *Пароль* также является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для аутентификации субъектов.

В ***симметричных криптосистемах*** для зашифрования и для расшифрования используется один и тот же ключ.

В ***асимметричных системах (системах с открытым ключом)*** используются два ключа - *открытый (публичный)* и *закрытый (секретный),* которые математически связаны друг с другом. Информация зашифровывается с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины *распределение ключей* и *управление ключами* относятся к процессам системы обработки информации.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.

Зашифрованием данных называется процесс преобразования открытых данных в зашифрованные с помощью шифра, а ***расшифрованием*** данных –

процесс преобразования закрытых данных в открытые с помощью шифра. Вместо термина «открытые данные» употребляются термины *открытый текст* и *исходный текст,* а вместо «зашифрованные данные» – *шифрованный текст.*

Дешифрование – процесс преобразования закрытых данных в открытые при неизвестном ключе и/или неизвестном алгоритме, т.е. методами криптоанализа.

Шифрование процесс зашифрования или расшифрования данных. (синоним зашифрования). Однако неверно в качестве синонима шифрования использовать термин *«кодирование»* (а вместо *«шифра» - «код»),* т.к. под кодированием понимают представление информации в виде знаков (букв алфавита).

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

Гамма шифра – псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для зашифрования открытых данных и расшифрования зашифрованных данных.

Имитозащита – защита от навязывания ложных данных. Для обеспечения имитозащиты к зашифрованным данным добавляется имитовставка, представляющая собой последовательность данных фиксированной длины, полученную по определенному правилу из открытых данных и ключа.

Криптографическая защита – это защита данных с помощью криптографического преобразования, под которым понимается преобразование данных *шифрованием* и (или) выработкой *имитовставки*.

Синхропосылка – исходные открытые параметры алгоритма криптографического преобразования.

Уравнение зашифрования (расшифрования) – соотношение, описывающее процесс образования зашифрованных (открытых) данных из

открытых (зашифрованных) данных в результате преобразований, заданных алгоритмом криптографического преобразования.

Требования к криптографическим системам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: *высокая производительность, простота, защищенность* и т.д. Программная реализация более *практична,* допускает известную *гибкость в использовании*.

Независимо от способа реализации для современных криптографических систем защиты информации сформулированы следующие общие требования:

– стойкость шифра противостоять криптоанализу должна быть такой, чтобы вскрытие его могло быть осуществлено только решением задачи полного перебора ключей либо должно выходить за пределы возможностей современных компьютеров (с учетом распараллеливания вычислений) или требовать создания использования дорогих вычислительных систем;

– криптостойкость обеспечивается не секретностью алгоритма, а секретностью ключа (разделяет криптосистемы **общего использования** (алгоритм доступен потенциальному нарушителю) и **ограниченного использования** (алгоритм держится в секрете));

– зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

– шифр должен быть стойким даже в случае, если нарушителю известно достаточно большое количество исходных данных и соответствующих им зашифрованных данных;

– незначительное изменение ключа или исходного текста должно приводить к существенному изменению вида зашифрованного текста;

– структурные элементы алгоритма шифрования неизменны;

– шифртекст не должен существенно превосходить по объему исходную информацию; дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

– ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

– не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

– любой ключ из множества возможных должен обеспечивать равную криптостойкость (обеспечение линейного (однородного) пространства ключей);

– время шифрования не должно быть большим;

– стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

3.3 Крипто анализ информации выводы.

Главным действующим лицом в криптоанализе выступает ***нарушитель*** (или ***криптоаналитик***) – лицо (группу лиц), целью которого является прочтение или подделка защищенных криптографическими методами сообщений.

В отношении нарушителя принимается ряд допущений, которые, как правило, кладутся в основу математических или иных моделей:

1. Нарушитель знает алгоритм шифрования (или выработки ЭЦП) и особенности его реализации в конкретном случае, но не знает секретного ключа.

2. Нарушителю доступны все зашифрованные тексты. Нарушитель может иметь доступ к некоторым исходным текстам, для которых известны

соответствующие им зашифрованные тексты.

3. Нарушитель имеет в своем распоряжении вычислительные, людские, временные и иные ресурсы, объем которых оправдана потенциальной ценностью информации, которая будет добыта в результате криптоанализа.

Попытку прочтения или подделки зашифрованного сообщения, вычисления ключа методами криптоанализа называют ***криптоатакой*** или *атакой на шифр.* Удачную криптоатаку называют ***взломом***.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к расшифрованию без знания ключа (т.е. криптоатаке). Показатель криптостойкости – главный параметр любой криптосистемы. В качестве показателя криптостойкости можно выбрать:

- количество всех возможных ключей или вероятность подбора ключа за заданное время с заданными ресурсами;
- количество операций или время (с заданными ресурсами), необходимое для взлома шифра с заданной вероятностью;
- стоимость вычисления ключевой информации или исходного текста.

Эти показатели должны учитывать уровень возможной криптоатаки.

Но эффективность защиты информации криптографическими методами зависит не только от криптостойкости шифра, но и от множества других факторов, включая вопросы реализации криптосистем и *человеческий фактор.* Например, подкуп конкретного человека, в руках которого сосредоточена необходимая информация, может стоить на несколько порядков дешевле, чем создание суперкомпьютера для взлома шифра.

Современный криптоанализ опирается на теорию вероятностей и математическую статистику, алгебру, теорию чисел, теория алгоритмов и ряд других. Все методы криптоанализа укладываются в четыре направления.

1.*Статистический криптоанализ* (исследует возможности взлома криптосистем на основе изучения статистических закономерностей исходных и зашифрованных сообщений. Его применение осложняется

предварительным сжатием информации перед шифрованием подвергается сжатию, или в случае гаммирования используются псевдослучайные последовательности большой длины).

2.*Алгебраический криптоанализ* **(**занимается поиском математически слабых звеньев криптоалгоритмов. Например в 1997 году в эллиптических системах был выявлен класс ключей, существенно упрощавший криптоанализ).

3.***Дифференциальный (или разностный) криптоанализ*** **(**Основан на анализе зависимости изменения шифрованного текста от изменения исходного текста (впервые использован Мерфи, улучшен Бихэмом и Шамиром для атаки на DES)).

4.***Линейный криптоанализ.*** **(**Метод, основанный на поиске линейной аппроксимации между исходным и шифрованным текстом. Предложен Мацуи, впервые применен при взломе DES.).

Опыт взломов криптосистем показывает, что главным методом остается «лобовая» атака – проба на ключ.

Принято различать несколько *уровней криптоатаки* в зависимости от объем информации, доступной криптоаналитику. Выделяют три уровня криптоатаки по нарастанию сложности.

Атака по шифрованному тексту (Уровень КА1) **–** Нарушителю доступны все или некоторые зашифрованные сообщения.

Атака по паре «исходный текст - шифрованный текст». (Уровень КА2) **–** нарушителю доступны все или некоторые зашифрованные сообщения и соответствующие им исходные сообщения.

Атака по выбранной паре «исходный текст - шифрованный текст». (Уровень КА3) **–** Нарушитель имеет возможность выбирать исходный текст, получать для него шифрованный текст и на основе анализа зависимостей между ними вычислять ключ.

Современные криптосистемы обладают достаточной стойкостью даже к атакам уровня КА3 (нарушителю доступно по сути шифрующее устройство).

Классификация методов криптографического закрытия информации

В настоящее время известно большое число методов криптографического закрытия информации. Классификация методов шифрования (криптоалгоритмов) может быть осуществлена по следующим признакам:

по типу ключей: симметричные криптоалгоритмы; асимметричные криптоалгоритмы;

по размеру блока информации: потоковые шифры; блочные шифры;

по характеру воздействий, производимых над данными: метод замены (перестановки), метод подстановки; аналитические методы, аддитивные методы (гаммирование), комбинированные методы.

Кодирование может быть смысловое, символьное, комбинированное.

Закрытие информации другими способами может достигаться с помощью стеганографии, сжатия/расширения, рассечения/разнесения.

Выводы

В работе рассмотрены история развития дисциплины, связь с другими отраслями науки и техники, введены основные понятия и определения дисциплины, а также обоснованы принципы и требования к организации систем информационной безопасности.

Изучены вопросы администрирования МЭ, политика администрирования паролей, активный аудит, а также улаживание происшествий с безопасностью и контроль за импортом программ.

Таким образом, одним из путей решения “информационного голода”, своевременного получения, передачи и обмена информации с научными учреждениями и организациями, является организация АП ИВС оп, позволяющая решить проблему своевременного получения нужной информации общего пользования, между научными организациями и центрами не только военного ведомства и не только учреждениями России.

Миссия обеспечения информационной безопасности трудна, во многих случаях невыполнима, но всегда благородна.

В диссертации рассмотрены вопросы криптографической защиты информации, введены основные понятия и определения, а также рассмотрены алгоритмы применяемых шифров и проведен их сравнительный анализ.

Литература

Основная

1. Галатенко В.А. Основы информационной безопасности. М.:ИНТУИТ.РУ. – 2003. с.15-26.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах. М.: «Логос» – 2001. с. 8-16
3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: «Горячая Линия – Телеком» – 2001. с. 5-14.
4. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности – М.: Радио и связь - 2000.- с. 22-24.
5. Галатенко В.А. Основы информационной безопасности. М.:ИНТУИТ. РУ. – 2003. с. 175-193, 227-237.
6. Завгородний В.И. Комплексная защита информации в компьютерных системах. М.: «Логос» – 2001. с. 179-209.
7. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: «Горячая Линия – Телеком» – 2001. с.40-49.
8. Галатенко В.А. Основы информационной безопасности. М.:ИНТУИТ.РУ. – 2003. с. 242-270.
9. Инструкция по защите информации от несанкционированного доступа при подключении и использовании пользователями ИВС.
10. Руководство по обеспечению безопасности информации от несанкционированного доступа на объектах вычислительной техники ВС.
11. Специальные требования и рекомендации по защите информации, обрабатываемой ТС передачи и обработки информации в РФ.
12. Руководство по организации ПД ИТР в РФ.

13. Галатенко В.А. Основы информационной безопасности. М.:ИНТУИТ.РУ. – 2003. с. 201-208.

14. Завгородний В.И. Комплексная защита информации в компьютерных системах. М.: «Логос» – 2001. с. 133-158

15. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: «Горячая Линия – Телеком» – 2001. с. 52-82.

16. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – Учебное пособие для ВУЗов.- М.: «Горячая Линия – Телеком» – 2000. – с.197–272.

Дополнительная

1. Грибанов В.П., Калмыкова О.В., Сорока Р.И. Основы алгоритмизации и программирования, М., Изд.центр ЕАОИ.-2008.

2. Цветкова М. С., Великович Л. С. Информатика и ИКТ. -М.: Изд-во «Академия», 2011.

3. Фаронов В.В. Turbo Pascal 7.0 Учебный курс/– М.: КноРус, 2011.

4. Алексеев Е.Р., Чеснокова О.В. Турбо Паскаль 7.0 - 2 изд., НТ Пресс, 2007.

5. Вирт Н. Алгоритмы и структуры данных. СПб, Невский Диалект,2005.

6. Иванова Г.С. Основы программирования: Учебник для вузов. - М.: Изд-во МГТУ им. Н.Э.Баумана,2002.

7. Иванова Г.С. Ничушкина Т.С., Пугачёв Объектно-ориентированное программировани: Учебник для вузов. - М.: Изд-во МГТУ им. Н.Э.Баумана,2001.

8. Немнюгин С.А. Turbo Pascal. - СПб: Питер, 2003.

9. Семакин И. Г., Шестаков А. П. Основы алгоритмизации и программирования. -М. : Изд-во «Академия» 2008 г.

10. С.В.Симонович. Информатика. Базовый курс./ Учебник для вузов. 3-е изд. – СПб.: Питер, 2013.

11. Экономическая информатика / Под ред. П.В. Конюховского, Д.Н. Колесова. СПб.: Питер, 2000.

12. Информатика./Под ред. Н.В. Макаровой. М.: Финансы и статистика, 2011.

13. Информатика: Учебник для экономических специиальностей высших учебных заведений / Под ред. Н.В. Макаровой. М.: Финансы и статистика, 2011.

14. Н.В.Макарова., В.Б.Волков Информатика. /Учебник для вузов. Стандарт третьего поколения. СПб.: Питер, 2011

15. А.С.Грошев. Информатика. /Учебник для вузов. Изд-во АГТУ, Архангельск, 2010

16. А.Н.Степанов. Информатика. /Учебник для вузов. 6-е изд. – СПб.: Питер, 2010

17. А.Н.Степанов. Архитектура вычислительных систем и компьютерных сетей. СПб.: Питер, 2007

18. А.А.Забуга. Теоретические основы информатики. /Учебное пособие. Стандарт третьего поколения. СПб.: Питер, 2014

19. А.Д.Хомоненко, В.М.Цыганков, М.Г.Мальцев. Базы данных. Учебник для высших учебных заведений. 6-е изд., Изд-во: Корона-век 2009г.

20. Самоучитель Access 2013 / Ю. Б. Бекаревич, Н. Пушкина. — Санкт-Петербург: БХВ-Петербург, 2014.

21. Самоучитель Microsoft Windows 8/ Д. Колисниченко СПб.: БХВ-Петербург, 2013.

22. Самоучитель Сеть своими руками /А.Поляк-Брагинский. 3-е изд. СПб.: БХВ-Петербург, 2013.