МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

С.К. ГАНИЕВ, З.Т. ХУДОЙКУЛОВ, Н.Б. НАСРУЛЛАЕВ

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Рекомендовано Координационным советом Министерства высшего и среднего специального образования Республики Узбекистан в качестве учебного пособия

Под редакцией профессора С.К. Ганиева

ТАШКЕНТ
«IQTISOD-MOLIYA»
2021

УДК: 004.056
ББК: 32.965.9

Рецензенты: *канд. техн. наук, доц*. **К.А. Ташев;**
канд. техн. наук **О.П. Ахмедова**

Г 19 **Основы кибербезопасности:** Учебное пособие / С.К. Ганиев, З.Т. Худойкулов, Н.Б. Насруллаев; – Т.: «Iqtisod-Moliya», 2021. – 240 с.

В учебном пособии рассматриваются вопросы кибербезопасности и ее основные понятия, архитектура, стратегия и политика кибербезопасности, криптографическая защита информации, контроль доступности, методы обеспечения доступности, сетевая безопасность, безопасность программных средств, а также теоретические и практические основы киберпреступности, киберправа, киберэтики и безопасность человеческой деятельности.

Пособие рекомендовано студентам, обучающимся по направлениям 5330300 – «Информационная безопасность», 5330500 – «Компьютерный инжиниринг (Компьютерный инжиниринг, IT-сервис, Мультимедийные технологии)», 5330600 – «Программный инжиниринг», 5350100 – «Телекоммуникационные технологии (Телекоммуникация, телерадиовещание, мобильные системы)», 5350200 – «Телевизионные технологии (Аудиовизуальные технологии, системы и приложения телестудии)», 5350300 – «Экономика и менеджмент в сфере информационно-коммуникационных технологий», 5350400 – «Профессиональное образование в сфере информационно-коммуникационных технологий», 5350500 – «Технология почтовой связи» и 5350600 – «Информатизация и библиотечное дело», а также может быть полезно широкому кругу специалистов, деятельность которых связана с обеспечением информационной безопасности.

УДК: 004.056
ББК: 32.965.9

ISBN 978-9943-13-9 88-6

ВВЕДЕНИЕ

Новые технологии, электронные услуги стали неотъемлемой частью нашей повседневной жизни. Поскольку общество становится все более зависимым от информационных и коммуникационных технологий, защита и использование этих технологий имеют решающее значение для национальных интересов.

По этой причине, для обеспечения кибербезопасности каждая организация занимается вопросами кибербезопасности, и для ознакомления сотрудников со знаниями о кибербезопасности организуются серии семинаров и тренингов. Ярким примером этого является то, что кибербезопасность как предмет преподается в высших учебных заведениях.

Наряду с развитием информационных технологий в республике особое внимание уделяется информационной безопасности, в частности, устранению проблем, связанных с компьютером в органах хозяйственного и государственного управления. В стратегии действий по дальнейшему развитию Республики Узбекистан на 2017-2021 годы поставлены задачи, в том числе особое внимание уделяется вопросам «...обеспечение информационной безопасности и модернизация системы защиты информации, своевременное и адекватное реагирование на угрозы в сфере информации» и выявление киберпреступности. Кроме того, Указом Президента Узбекистана «О государственной программе по реализации стратегии действий в «Год развития науки, просвещения и цифровой экономики» определены задачи «разработки национальной стратегии и проекта Закона о кибербезопасности до 1 сентября 2020 года». При реализации этих задач одним из важных аспектов, на который следует обратить внимание, является разработка учебных пособий в сфере кибербезопасности.

В первой главе пособия рассмотрены задачи и основные понятия предмета основы кибербезопасности, область его применения и вопросы человеческого фактора в кибербезопасности. Также затронуты вопросы киберпреступности, киберзаконы и киберэтики, приведена информация о видах наказаний, налагаемых за киберпреступность.

Вторая глава посвящена фундаментальным вопросам кибербезопасности, а также информации об архитектуре, стратегии и порядке реализации политики кибербезопасности.

В третьей главе рассмотрены основные понятия в области криптографической защиты информации, симметричные криптосистемы, криптосистемы с открытым ключом, методы обеспечения целостности данных, шифрования дисков и файлов, а также методы безопасного удаления данных.

Четвертая глава пособия посвящена контролю доступа, где представлены методы аутентификации, методы физического и логического управления данными. Описаны широко применяющиеся модели управления логическим доступом и рекомендации по их использованию.

Пятая глава посвящена сетевой безопасности, в которой рассматриваются проблемы безопасности в сети и использование межсетевых экранов, виртуальных защищенных сетей и других средств, для их устранения. Кроме того, рассмотрены вопросы безопасности и управления рисками в беспроводных сетях.

В шестой главе представлены данные о свойстве доступности и ее важности для системы, методы резервного копирования и восстановления данных. Поскольку процедура аудита считается важной для доступности системы, важно ознакомиться с порядком регистрации событий для ОС Windows.

Седьмая глава посвящена безопасности программных средств и описываются проблемы безопасности в программном обеспечении и фундаментальные принципы их предотвращения. Приведена подробная информация о вредоносных программных средствах, предназначенных для повреждения системы, их анализе и современных антивирусных программных средствах.

ГЛАВА 1. КИБЕРБЕЗОПАСНОСТЬ. ОБЩИЕ СВЕДЕНИЯ

1.1. Основные понятия кибербезопасности

Развитие современных методов обработки, передачи и сбора информации приводит к увеличению угроз, связанных с потерей, повреждением и разглашением пользовательской информации. Поэтому обеспечение информационной безопасности в компьютерных системах и сетях является одним из ведущих направлений развития информационных технологий.

Информационная безопасность основана на реальных образах. Есть люди, которые осуществляют легальную деятельность в жизни, как показано на рис. 1.1 в образе *Алисы* и *Боба*. Однако, есть и те, кто заинтересован деятельностью этих людей, мешающих их работе, и они изображены в образе *Триди*. Образ Триди олицетворяет людей, преследующих все корыстные побуждения.

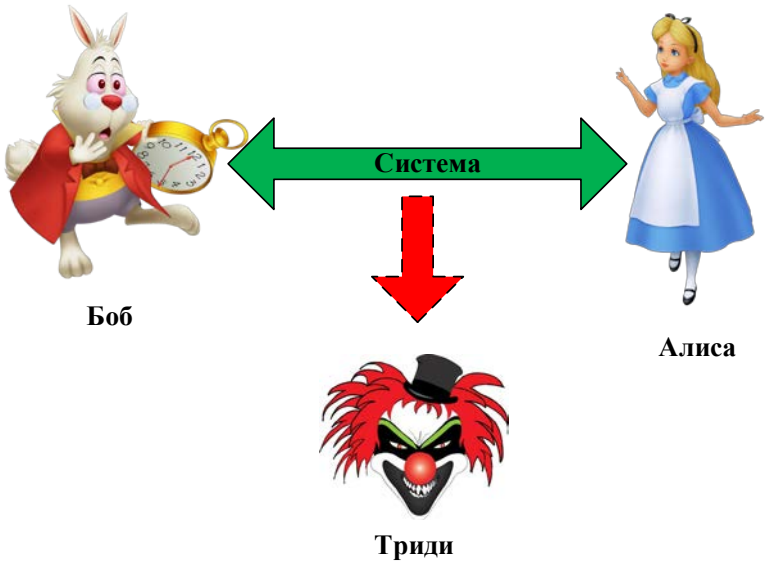


Рис.1.1. **Жизненные образы информационной безопасности**

Рассмотрим жизненный сценарий для освещения следующих разделов учебного пособия. Этот жизненный сценарий называется *онлайн банк Алисы (ОБА)*. Согласно нему, Алиса осуществляет предпринимательскую деятельность в сфере онлайн-банкинга. В чем заключается проблема безопасности Алисы в данном сценарии? А проблема Боба, который является клиентом Алисы? Проблемы безопасности Алисы и Боба одинаковы? Какие существуют проблемы безопасности с точки зрения Триди? Ответы на эти вопросы приводятся в следующих разделах.

Познакомимся с некоторыми понятиями, имеющими отношение к защите информации и информационной безопасности в компьютерных системах и сетях.

Кибербезопасность – в настоящее время является одним из новых введенных понятий, и существуют различные определения, данные ей. В частности, в источнике CSEC2017 Joint Task Force дано следующее определение кибербезопасности: ***кибербезопасность*** *– область знаний, основанная на вычислениях, включающая технологии, людей, информацию и процессы для того, чтобы гарантировать надлежащее выполнение действий в условиях, в которых находятся злоумышленники. Она включает в себя создание, реализация, анализ и тестирование безопасных компьютерных систем. Кибербезопасность – комплексная область знаний в образовании, которая включает в себя правовые аспекты, политику, человеческий фактор, этику и управление рисками.*

Организация *Cisco*, осуществляющая свою деятельность в области сетевых технологий, описала кирбербезопасность следующим образом: *Кибербезопасность – практика защиты систем, сетей и программ от цифровых атак. Эти кибератаки обычно нацелены на управление, замену или удаление конфиденциальной информации; взимание с пользователей денег; нарушение нормальной работы. В настоящее время реализация эффективных мер кибербезопасности с практической стороны становится все более сложной из-за большого количества устройств и количества их типов, чем людей, а также потенциала злоумышленников.*

Потребность в области знаний о кибербезопасности стала возникать с разработкой первого мэйнфрейм компьютера, где реализованы многоуровневые меры безопасности для защиты данных устройств и их функций. Растущая потребность в национальной безопасности приводит к появлению комплексных и технологически сложных надежных мер безопасности.

В настоящее время, каждый специалист, работающий в сфере информационных технологий, должен обладать фундаментальными знаниями в области кибербезопасности. Структуру предметной области кибербезопасности можно описать следующим образом (рис. 1.2).

Рис.1.2. **Структура предметной области кибербезопасности**

Существуют разные подходы к определению основных терминов кибербезопасности. В частности, в источнике CSEC2017 JTF перечислены следующие 6 терминов кибербезопасности:

Конфиденциальность – свойство информации, состоящее в том, что она не может быть обнаружена или сделана доступной без разрешения отельным лицам, модулям или процессам. Конфиденциальность занимается защитой информации от несанкционированного «считывания». В сценарии ОБА для Боба очень важна конфиденциальность. То есть Боб не хочет, чтобы Триди знал, сколько денег у него на балансе. По этой причине для Боба важно обеспечить конфиденциальность информации о балансе.

Целостность – свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому физическому её состоянию). Целостность занимается защитой информации от несанкционированной «записи» (т.е. изменения информации) или, по крайней мере, определения того, была ли она изменена. В сценарии ОБА необходимо защитить

целостность банковского счета Алисы от Триди. Например, Боб должен защитить себя от изменения баланса на его счете или увеличения баланса на счете Алисы.

Здесь необходимо обратить внимание на то, что конфиденциальность и целостность – это не одно и то же понятие. Например, даже если Триди не может прочитать какую-либо информацию, он может незаметно ее изменить.

Доступность – свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта. Доступность занимается защитой информации (или системы) от несанкционированного «сбоя». В сценарии ОБА неспособность Боба воспользоваться веб-сайтом ОБА является проблемой доступности для банка Алисы и Боба. Причина в том, что в этом случае Алиса не может получать прибыль от денежных переводов, а Боб не может реализовать свой бизнес. Наиболее распространенной из атак, направленных на нарушение доступности, является атака, принуждающая на отказ в обслуживании (Denial of Service, DoS).

Риск – потенциальная выгода или убыток, в общем случае риск возникает, когда вероятность наступления события добавляется к какой-либо ситуации. ISO определяет риск как «влияние неопределенности на цели».

Например, рассмотрим процесс поступления в университет. В целом этот процесс сам по себе не считается риском. Только после подачи абитуриентом документов и вступительных экзаменов он может поступить или не поступить на учебу. Это, в свою очередь, приводит к риску быть принятым или не быть принятым.

В кибербезопасности или информационной безопасности риски рассматриваются критично.

Мыслить, как злоумышленник – процесс мышления пользователя законного как злоумышленника, чтобы предотвратить возможного риска.

Системное мышление – мыслительный процесс, учитывающий взаимодействие социальных и технических ограничений с целью обеспечения гарантированных действий.

Кроме того, следующие понятия также важны при изучении сферы кибербезопасности.

Безопасность информации – состояние информации, при котором исключаются случайные или преднамеренные

несанкционированные воздействия на информацию или несанкционированное ее получение. Или состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающие сохранение таких ее качественных характеристик (свойств) как секретность (конфиденциальность), целостность и доступность.

Защита информации – включает в себя комплекс мероприятий, направленных на обеспечение информационной безопасности. На практике под этим понимается поддержание целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Актив – информация или ресурсы, подлежащие защите. Или, все, что имеет ценность для организации.

Угроза – нежелательное событие, которое может нанести ущерб системе или организации. Или, угроза – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Угроза нацелена на активы организации. Например, если актив – хранимый документ, принадлежащий предприятию, то угроза может быть направлена против помещения, где хранится этот документ.

Уязвимость – недостаток в активах или системе управления организации, позволяющий реализовать одну или несколько угроз.

Средство управления – действие, изменяющее риск, результат которого влияет на изменение уязвимости или угрозы. Кроме того, само средство управления может иметь уязвимость, которая может быть использована различными угрозами. Например, огнетушители можно рассматривать как средство управления для защиты информации в бумажной форме, хранящейся в организации, от пожара. В случае пожара, действия сотрудников и меры, принимаемые для предотвращения пожара, также могут рассматриваться как средство управления. А состояние неисправности системы пожаротушения рассматривается как недостаток в средстве управления.

Различие между информационной безопасностью и кибербезопасностью. Термины «кибербезопасность» и «информационная безопасность» часто используются как синонимы. В то время как некоторые рассматривают

кибербезопасность как синоним понятий информационной безопасности, безопасности информационных технологий и (информационного) управления рисками, некоторые рассматривают кибербезопасность как техническую концепцию, связанную с национальной безопасностью, которая включает защиту от компьютерных преступлений и критических инфраструктур, особенно в государственном секторе. Хотя известны случаи адаптации сотрудников в различных отраслях к своим целям, существуют некоторые важные различия между понятиями информационной безопасности и кибербезопасности.

Сфера *информационной безопасности* занимается защитой интеллектуальных прав независимо от формы выражения информации (бумажной, электронной и человеко-мыслительной, вербальной и визуальной). *Кибербезопасность* занимается защитой информации в электронном виде (во всех случаях, от сети до устройства, хранящейся, передаваемой и обрабатываемой во взаимосвязанных системах). Кроме того, финансируемые государством атаки и продвинутые постоянные угрозы (Advanced persistent threats, APT) также относятся к кибербезопасности. Проще говоря, пониман,ие кибербезопасности как одного из направлений информационной безопасности помогает понять ее правильно.

Области знаний кибербезопасности. Согласно источнику CSEC2017 JTF, кибербезопасность делится на 8 областей знаний, каждая из которых подразделяется на подсекторы (рис. 1.3).

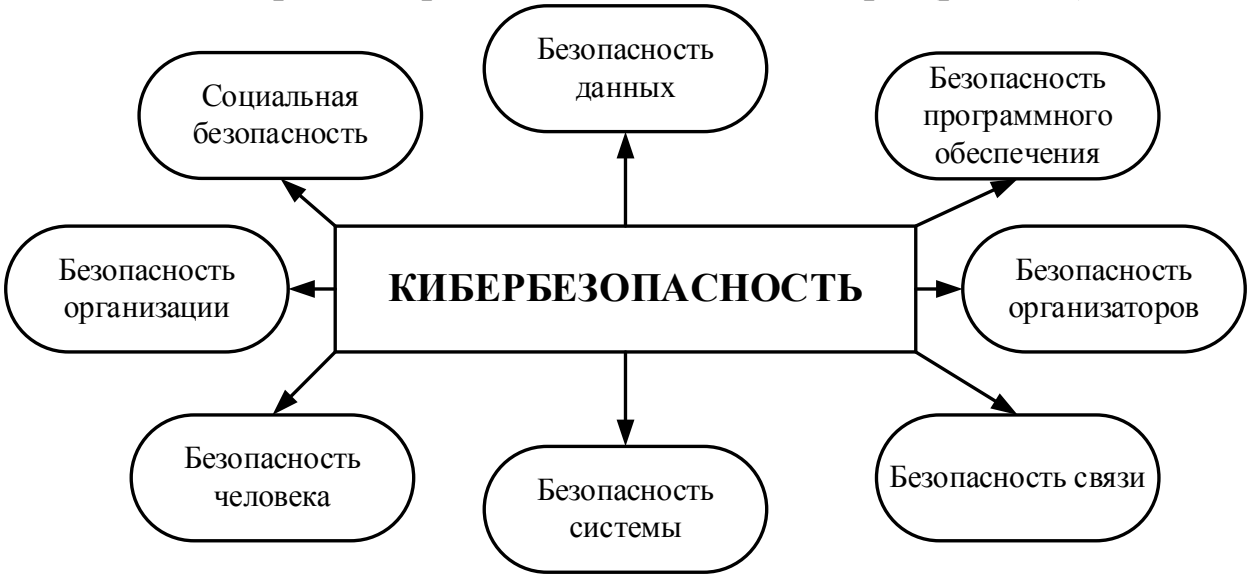


Рис.1.3. **Области знаний кибербезопасности**

Целью области знаний «*Безопасность данных*» является обеспечение защиты при хранении, обработке и передаче данных. Для полной реализации защиты в данной области знаний используются математические и аналитические алгоритмы.

Область знаний *«Безопасность программного обеспечения»* обращает внимание на процесс разработки и использования программных средств, обеспечивающих безопасность используемой системы или информации.

Область знаний *«Организационная безопасность»* фокусируется на проектировании, закупке, тестировании, анализе и обслуживании интегрированных компонентов в больших системах. Системная безопасность иногда отличается от организационной безопасности. Организационная безопасность зависит от того, как система спроектирована, построена, приобретена, подключена к другим компонентам, а также как она работает и поддерживается.

Область знаний *«Безопасность связи»* ориентирована на коммуникацию между организаторами, воплощая в себе физическую и логическую связь.

Область знаний *«Безопасность системы»* фокусируется на аспектах системной безопасности, состоящих из организаторов, соединений и программного обеспечения. Чтобы понять безопасность системы, необходимо не только понимать ее компоненты и их связи, но и учитывать целостность. То есть, это требует тщательного пересмотра системы. Данная область знаний, наряду с областями знаний «Организационная безопасность» и «Безопасность связи», решает вопрос о безопасности соединений организаторов и их использовании в более высоких системах.

Область знаний «*Безопасность жизнедеятельности*» помимо изучения поведения человека, связанного с кибербезопасностью, фокусируется на защите данных и личности в организациях (например, сотрудников) и в личных жизненных ситуациях.

Область знаний «*Безопасность организации*» фокусируется на управлении рисками для защиты организации от угроз кибербезопасности и поддержки успешной деятельности организации.

Область знаний «*Социальная безопасность*» фокусируется на факторах кибербезопасности, которые в той или иной степени влияют на общество. Киберпреступность, законы, моральные

отношения, политика, личная жизнь и их взаимоотношения друг с другом являются основными понятиями в этой области знания.

Таким образом, можно сказать, что сфера кибербезопасности является необходимой сферой для специалистов в области информационных технологий.

1.2. Человеческий фактор в кибербезопасности

Пользователи считаются самой уязвимой точкой в системе кибербезопасности. Со стороны пользователей может быть нарушена любая степень безопасности, даже высокая. Например, предположим, что Боб хочет что-то купить в онлайн-магазине amazon.com. Для этого Боб может использовать веб-браузер для надежного подключения к Amazon с помощью протокола SSL (Secure Sockets Layer), опирающегося на различные криптографические методы. Этот протокол обеспечивает гарантированную безопасность при правильном выполнении всех необходимых действий. Однако, существуют несколько типов атак, направленных на этот протокол (атака «человек посередине» Man-in-the-middle attack), которые требуют «участия» пользователя для их реализации (рис. 1.4). Если пользователь выберет безопасный режим *(Вернуться к безопасной странице)*, то атака не состоится. Однако, если со стороны пользователя осуществится небезопасный выбор (*Перейти на сайт …. (небезопасно)*), то атака завершается успешно. Другими словами, даже когда используется протокол с высоким уровнем безопасности, безопасность может быть нарушена из-за неправильных действий пользователя.

Обычно пользователи стараются использовать легко запоминающиеся пароли. Однако, такое поведение повышает вероятность угадывания паролей для злоумышленника. С другой стороны, при использовании сложных паролей и хранении их в различных носителях (например, записи на бумаге), данная проблема еще больше усугубляется.

Эти примеры показывают, что из-за человеческого фактора проблемы безопасности могут возникать в разных местах и ситуациях. Можно привести много примеров проблем безопасности, возникающих из-за человеческого фактора. Однако, наиболее важным аспектом в представленных случаях является необходимость исключить человеческий фактор из «уравнения» с

точки зрения безопасности. Другими словами, системы, в которых не участвует человеческий фактор, более безопасны, чем системы, в которых он присутствует.

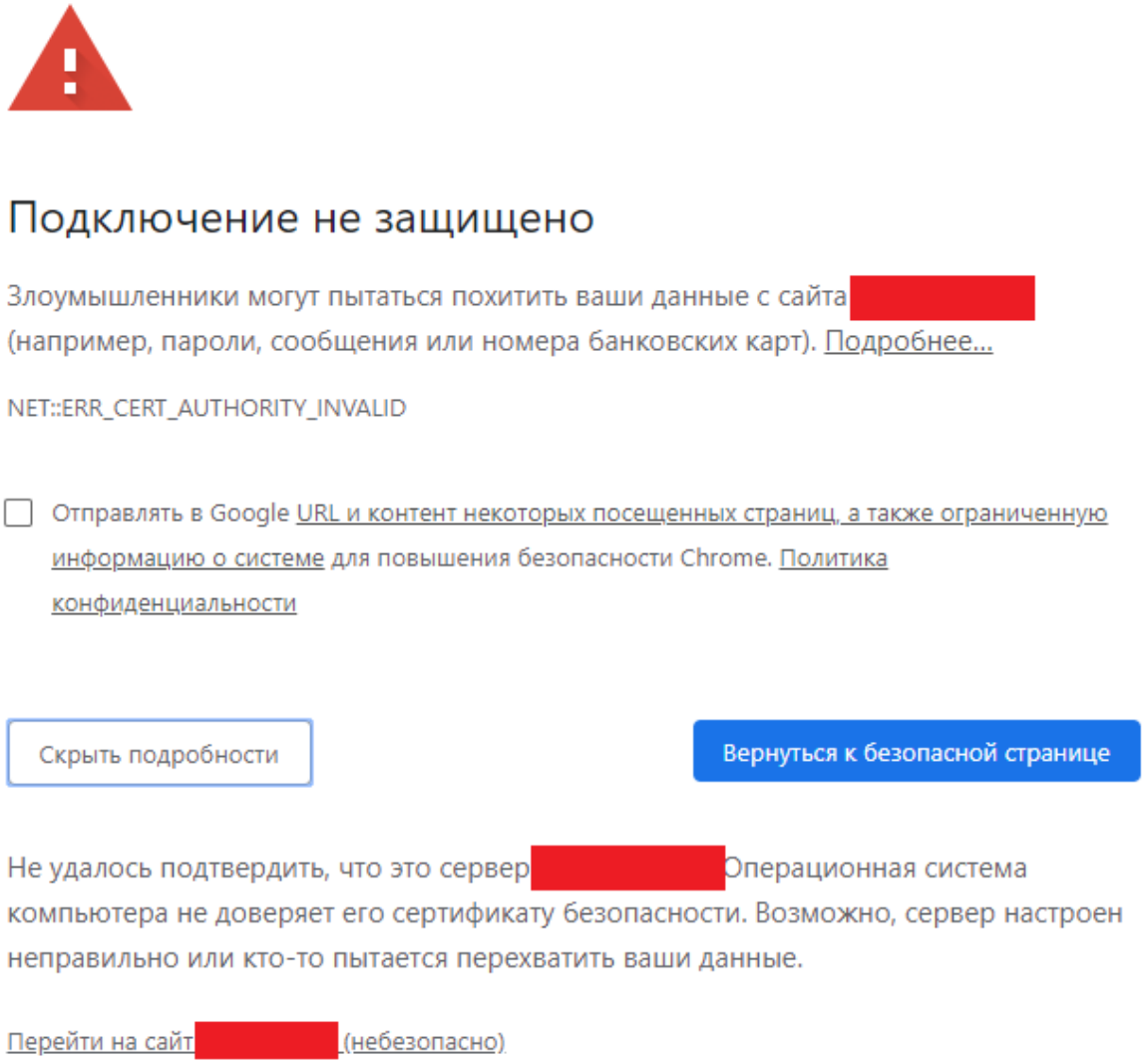


Рис.1.4. **Предупреждение о безопасности в протоколе SSL**

К наиболее важным человеческим факторам относятся:

- *недостаток знаний в области кибербезопасности* приводит к появлению большого количества открытых уязвимостей. Поскольку область кибербезопасности связана с традиционной безопасностью, быстрота необходимой технологической адаптации часто увеличивает число уязвимостей, которые могут возникнуть во многих случаях. С другой стороны, человеку не всегда достаточно владеть новейшими технологическими знаниями, связанными с отраслью;

- *недостаточность устранения рисков и сообщений о них* могут привести к повторным и неожиданным нарушениям кибербезопасности. Хотя люди обычно осознают, что существует серьезный риск для их организации, они не раскрывают его. В качестве основной причины приводят то, что риск непосредственно влияет на самого человека, его финансовое положение, или падение репутации человека при его раскрытии;

- *проблемы в культуре и взаимоотношениях могут быть вызваны* появлением недовольного и невнимательного сотрудника, который знает саму организацию или внутренние данные организации. Большинство проблем кибербезопасности являются внутренними, возникающими в результате различных разногласий между сотрудниками и неблагоприятной средой внутри организации. Эти причины в большинстве случаев приводят к серьезным проблемам, так как сотрудник хорошо осведомлен о внутренней структуре организации;

- *недостаточное финансирование занятий по безопасности* является причиной низкой осведомленности об управляемых рисках безопасности. Как правило, сотрудники предприятий данной сферы не изучают правила кибербезопасности самостоятельно. Поэтому необходимо будет донести до сотрудников правила кибербезопасности в форме специального обучения. Это требует со стороны организации финансирования достаточных средств на обучение безопасности;

- в результате *неоднородности точки регистрации* наблюдается неполноценное обеспечение безопасности. На практике является важным осуществлять контроль в единой точке для гарантированного обеспечения безопасности. Единая точка контроля безопасности более надежна, чем распределенная форма. Однако из-за сложности контроля безопасности в организациях управление обычно осуществляется распределенным образом;

- при обходе контроля безопасности на основе *социальной инженерии* данные получаются от пользователя с использованием традиционных методов шпионажа. Даже организация с лучшей системой кибербезопасности может столкнуться с угрозой социальной инженерии. В частности, пренебрежение личной информацией пользователей в различных социальных сетях приводит к резкому увеличению этого риска.

1.3. Киберпреступность, киберзаконы и киберэтика

Киберпреступность – действия отдельных лиц или групп, направленные на взлом систем компьютерной защиты, на хищение или разрушение информации в корыстных или хулиганских целях.

Для организации, столкнувшейся с кибератакой, киберпреступность может быть внутренней или внешней:

Внутренняя киберпреступность: осуществляется в сети или компьютерной системе лицом, которое знакомо с ними и имеет законное право использовать их. Данный вид киберпреступности обычно осуществляется обиженными и недовольными сотрудниками организации. И целью этих сотрудников может быть месть организации или ее руководителю, или жадность. Поскольку обиженный сотрудник хорошо знаком с ИТ-инфраструктурой, архитектурой и системой безопасности, данный вид преступления может нанести серьезный ущерб организации. Кроме того, киберпреступник получит доступ к сети организации. Поэтому в результате внутренней киберпреступности высока вероятность утечки конфиденциальной информации.

Внешняя киберпреступность: обычно осуществляется злоумышленником, нанятым извне или внутри организации. Данный вид киберпреступности приводит не только к финансовым потерям организации, но и к потере репутации. Поскольку атака осуществляется извне, злоумышленник начинает действие со сканирования ИТ-инфраструктуры организации и сбора связанной с ней информации. В частности, квалифицированный злоумышленник сначала начинает с анализа лог файла инструмента межсетевого экрана, используемого в организации. Поэтому сетевой администратор не должен предоставлять такую возможность злоумышленнику.

При осуществлении киберпреступности в качестве основной цели рассматриваются:

- незаконное присвоение денежных средств, ценных бумаг, кредитов, материальных ценностей, товаров, услуг, льгот, недвижимости, топливно-энергетических ресурсов и стратегического сырья;
- отказ от уплаты налогов и других сборов;
- легализация преступных доходов;

- подделка документов, штампов, печатей, бланков, личных выигрышных билетов;

- получение конфиденциальной информации в личных или политических целях;

- месть за предвзятое отношение администрации или коллег по работе;

- нарушение денежной системы страны в личных или политических целях;

- дестабилизация обстановки, территориально-административного устройства в стране;

- грабеж, уничтожение противника или нарушение правил деятельности учреждения, предприятия или системы в политических целях;

- демонстрация личной интеллектуальной способности или превосходство.

- Невозможно строго классифицировать виды киберпреступлений. Ниже приведены виды киберпреступности по отношению к области криминологии:

- экономическая компьютерная преступность;

- компьютерная преступность, направленная против конституционных прав и свобод человека и гражданина;

- компьютерная преступность против общественной и государственной безопасности.

На практике часто встречаются экономические компьютерные преступления. Они приносят преступникам миллионы долларов США нелегального дохода. Наиболее распространенное из них мошенничество в основном реализуется с помощью банковских счетов и банковских карт. В международной практике преступления, совершенные с использованием пластиковых карт, связаны с утерянными или украденными картами, созданием или использованием поддельных платежных карт, получением и незаконным использованием информации о банковском счете без предъявления карты, а также преступлениями, совершенными держателем карты.

Другой вид киберпреступности – «компьютерное пиратство», преступления, направленные против прав и свобод человека и гражданина. Эти преступления проявляются в незаконном копировании, использовании и распространении программного обеспечения. Это серьезно наносит ущерб правовым отношениям

(авторским правам), связанным с программным обеспечением и созданием базы данных. Кроме того, это приводит к огромным финансовым потерям для компаний, занимающихся программным обеспечением.

Как утверждает директор компании «Майкрософт Армения» Григор Барсегян, ущерб, нанесенный разработчикам «компьютерным пиратством», составляет 66 миллиардов долларов в год. По его словам, пользователи Армении в целях экономии своих денежных средств, сознательно пользовались программами, степень риска заражения вирусов которых является высокой.

Последний вид компьютерной преступности – компьютерные преступления против общественной или государственной безопасности, к ним относятся действия, направленные на государственную или общественную безопасность. Они часто связаны с нарушением правил передачи данных, системы обороны страны или ее компонентов.

Киберзаконы. Закон (право) – средство укрепления, развития и регулирования общественных отношений, которые являются важнейшими в интересах человека, общества и государства. Можно определить, на что направлен закон, в зависимости от отношения, на которое он направлен. Следовательно, законы могут иметь цели в различных областях. В общем названии законы, направленные на регулирование киберпреступности, называются киберзаконами.

Законодатели и правозащитники по всему миру предупреждают о необходимости принятия законов о киберпреступности, которые четко определяют киберпреступность и полностью поддерживают принятие кибер-доказательств. Участие страны в международном договоре вступает в силу только в том случае, если разработаны и утверждены внутренние законы, легализующие этот договор. В Европе, например, в 2004 году Совет Европы принял проект Договора о киберпреступности (также известного как Будапештская конвенция), который был предложен странам всего мира. Хотя большинство государств подписали этот Договор, лишь немногие из них имеют национальные законы, соответствующие этому договору.

К февралю 2020 года 106 (или 55%) государств-членов Организации Объединенных Наций в соответствии с Будапештской конвенцией разработали национальные законы о киберпреступности. Кроме того, в настоящее время развивающиеся

страны приняли определенные полномочия по расследованию киберпреступников и сбору необходимых для этого данных.

В частности, в проекте Указа Президента Республики Узбекистан «О государственной программе по реализации стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017-2021 годах в «Год развития науки, просвещения и цифровой экономики»» также запланирована разработка проекта национальной стратегии по кибербезопасности на 2020-2023 годы и закона «О кибербезопасности».

Согласно документу, обеспечение безопасности, межнационального согласия и религиозной толерантности, а также в сфере внешней политики:

До 1 сентября 2020 года будут приняты меры по формированию правовой базы кибербезопасности, включая разработку национальной стратегии кибербезопасности на 2020-2023 годы и проект закона «О кибербезопасности».

В проекте предусмотрено:

- защита системы информационно-коммуникационных технологий от современных киберугроз, внедрение современных механизмов кибербезопасности для различных уровней систем;
- определение прав и обязанностей государственных органов, предприятий и организаций в области кибербезопасности, координация их деятельности;
- унификация нормативно-правовых документов в этой сфере.

Киберзаконы формируются на основе национальных правовых норм каждого государства или являются их частью. Ниже перечислены пункты, касающиеся предотвращения и регулирования киберпреступности в законодательстве нашей республики.

Национальные законы. 12 декабря 2002 года принят Закон Республики Узбекистан № 439-II «О принципах и гарантиях свободы информации». Этот закон состоит из 16 статей, в которых определено следующее:

Статья 1. Основные задачи настоящего Закона

Основными задачами настоящего Закона являются обеспечение соблюдения принципов и гарантий свободы информации, реализации права каждого свободно и беспрепятственно искать, получать, исследовать, распространять, использовать и хранить

информацию, а также обеспечение защиты информации и информационной безопасности личности, общества и государства.

Статья 4. Свобода информации

В соответствии с Конституцией Республики Узбекистан каждый обладает правом беспрепятственно искать, получать, исследовать, распространять, использовать и хранить информацию.

Доступ к информации может быть ограничен только в соответствии с законом и в целях защиты прав и свобод человека, основ конституционного строя, нравственных ценностей общества, духовного, культурного и научного потенциала, обеспечения безопасности страны.

Статья 6. Открытость и гласность информации

Информация должна быть открытой и гласной, за исключением конфиденциальной.

К конфиденциальной информации не относятся:

- акты законодательства о правах и свободах граждан, порядке их реализации, а также устанавливающие правовой статус органов государственной власти и управления, органов самоуправления граждан, общественных объединений и других негосударственных некоммерческих организаций;

- сведения об экологической, метеорологической, демографической, санитарно-эпидемиологической, чрезвычайной ситуации, и другая информация, необходимая для обеспечения безопасности населения, населенных пунктов, производственных объектов и коммуникаций;

- сведения, имеющиеся в открытых фондах информационно-библиотечных учреждений, архивов, ведомственных архивов и информационных систем юридических лиц, функционирующих на территории Республики Узбекистан.

Органы государственной власти и управления, органы самоуправления граждан, общественные объединения и другие негосударственные некоммерческие организации обязаны передавать средствам массовой информации сообщения о событиях, фактах, явлениях и процессах, представляющих интерес для общества, в порядке, установленном законодательством.

Статья 10. Отказ в предоставлении информации

Отказ в предоставлении запрашиваемой информации возможен, если она является конфиденциальной или в результате ее

раскрытия может быть причинен ущерб правам и законным интересам личности, интересам общества и государства.

Уведомление об отказе в предоставлении запрашиваемой информации направляется обратившемуся с запросом лицу в пятидневный срок с даты его получения.

В уведомлении об отказе должна быть указана причина, по которой запрашиваемая информация не может быть предоставлена.

Собственник, владелец конфиденциальной информации, обязан уведомлять лиц, запрашивающих информацию, о действующих ограничениях доступа к этой информации.

Лица, которым неправомерно отказано в предоставлении информации, а также лица, получившие на свой запрос недостоверную информацию, имеют право на возмещение причиненного им материального ущерба или компенсацию морального вреда в установленном законом порядке.

Статья 11. Защита информации

Защите подлежит любая информация, противоправное обращение с которой может причинить ущерб ее собственнику, владельцу, пользователю и иному лицу.

Защита информации осуществляется в целях:

- предотвращения угроз безопасности личности, общества и государства в информационной сфере;
- сохранения конфиденциальности информации, предотвращения ее утечки, хищения, утраты;
- предотвращения искажения и фальсификации информации.

Статья 13. Информационная безопасность личности

Информационная безопасность личности обеспечивается путем создания необходимых условий и гарантий свободного доступа к информации, защиты тайны частной жизни, защиты от противоправных информационно-психологических воздействий.

Информация о персональных данных физических лиц относится к категории конфиденциальной информации.

Не допускается сбор, хранение, обработка, распространение и использование информации о частной жизни, а равно информации, нарушающей тайну частной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме случаев, установленных законодательством.

Запрещается использование информации о физических лицах в целях причинения им материального ущерба и морального вреда, а также воспрепятствования в реализации их прав, свобод и законных интересов.

Юридические и физические лица, получающие, владеющие и использующие информацию о гражданах, несут предусмотренную законом ответственность за нарушение порядка использования этой информации.

Средства массовой информации не вправе раскрывать источник информации или автора, подписавшегося псевдонимом, без их согласия. Источник информации или имя автора могут быть раскрыты только по решению суда.

Статья 14. Информационная безопасность общества

Информационная безопасность общества достигается путем:

- обеспечения развития основ демократического гражданского общества, свободы массовой информации;
- недопущения противоправного информационно-психологического воздействия на общественное сознание, манипулирования им;
- сохранения и развития духовных, культурных и исторических ценностей общества, научного и научно-технического потенциала страны;
- создания системы противодействия информационной экспансии, направленной на деформацию национального самосознания, отрыв общества от исторических и национальных традиций и обычаев, дестабилизацию общественно-политической обстановки, нарушение межнационального и межконфессионального согласия.

Статья 15. Информационная безопасность государства

Информационная безопасность государства обеспечивается путем:

- реализации мер экономического, политического, организационного и иного характера по противодействию угрозам безопасности в информационной сфере;
- защиты государственных секретов и государственных информационных ресурсов от несанкционированного доступа к ним;

- интеграции Республики Узбекистан в мировое информационное пространство и современные телекоммуникационные системы;

- защиты от распространения информации, содержащей публичные призывы к насильственному изменению конституционного строя, нарушению территориальной целостности, суверенитета Республики Узбекистан, захвату власти или отстранению от власти законно избранных или назначенных представителей власти и совершению иных посягательств на государственный строй;

- противодействия распространению информации, содержащей пропаганду войны и насилия, жестокости, идей терроризма и религиозного экстремизма, направленной на разжигание социальной, национальной, расовой и религиозной вражды.

Статья 16. Ответственность за нарушение законодательства о принципах и гарантиях свободы информации

Лица, виновные в нарушении законодательства о принципах и гарантиях свободы информации, несут ответственность в установленном порядке.

Ответственность по борьбе с киберпреступностью в Республике Узбекистан перечислена ниже.

Кодекс Республики Узбекистан об административной ответственности:

Статья 155. Нарушение правил пользования информацией

-Нарушение правил пользования информацией и информационными системами, выразившееся в несанкционированном доступе в информационную систему с целью ее использования –

влечет наложение штрафа на граждан от одной третьей до одной, а на должностных лиц – от одной до трех базовых расчетных величин.

-То же правонарушение, повлекшее за собой нарушение функционирования информационных систем, а равно непринятие соответствующих мер защиты при включении информационных систем с ограниченным доступом в информационно-вычислительные сети —

влечет наложение штрафа на граждан от одной до трех, а на должностных лиц – от трех до пяти базовых расчетных величин.

-Незаконное включение информационных систем юридических и физических лиц в международные информационные сети, включение в них без принятия необходимых мер защиты, а равно незаконное получение от них информации –

влечет наложение штрафа на граждан от двух до пяти, а на должностных лиц – от пяти до семи базовых расчетных величин.

-Выпуск под своим именем чужой программы для электронно-вычислительных машин или базы данных либо незаконное воспроизведение или распространение таких произведений –

влечет наложение штрафа на граждан от одной до трех, а на должностных лиц – от трех до пяти базовых расчетных величин.

Статья 218. Незаконное изготовление и распространение продукции средств массовой информации

-Незаконное изготовление и распространение продукции средств массовой информации без их регистрации в установленном порядке либо после решения о прекращении их выпуска или издания –

влечет наложение штрафа от трех до пяти базовых расчетных величин с конфискацией печатной или иной продукции.

Уголовный кодекс Республики Узбекистан:

Статья 143. Нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений

-Умышленное нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений, совершенное после применения административного взыскания за такие же действия, – наказывается штрафом до двадцати пяти базовых расчетных величин или лишением определенного права до трех лет, или обязательными общественными работами до трехсот шестидесяти часов либо исправительными работами до трех лет.

Киберэтика – это философская область, связанная с компьютерами, которая изучает поведение пользователей, то для чего компьютеры запрограммированы, и как они влияют на людей и общество в целом. Вопросам киберэтики можно привести следующие примеры:

- допустимо ли передавать личную информацию о других людях в интернете (например, онлайн-статус или текущее местоположение по GPS)?

- нужно ли защищать пользователей от фейковой информации?

- кто владеет цифровыми данными (музыка, фильмы, книги, веб-страницы и т.д.) и какие права по отношению к ним имеют пользователи?

- в какой степени должны быть онлайн азартные игры и порнография в сети?

- должен ли Интернет быть доступным каждому?

Собственность. Споры об этике использования информации долгое время вызывали озабоченность в связи с концепцией собственности и привели к множеству конфликтов в области кибербезопасности. Споры о собственности возникают, когда право собственности нарушено или не определено.

Права интеллектуальной собственности. Постоянный рост Интернета и появление различных технологий сжатия данных (например, формата файлов mp3) проложили огромный путь для обмена файлами «peer-ro-peer». Эта возможность изначально была реализована с помощью таких приложений, как Napster, но теперь она используется в протоколах передачи данных, таких как BitTorrent. Хотя большая часть передаваемой музыки защищена авторским правом, этот файлообмен является незаконным.

В настоящее время большинство электронных медиафайлов (музыка, аудио и кинофильмы) распространяются среди общественности без соблюдения прав интеллектуальной собственности. Например, наблюдаются случаи, когда большинство бюджетных фильмов не могут покрыть собственные расходы из-за выхода «пиратской» версии фильма.

Такую же ситуацию можно увидеть в программном обеспечении. Например, хотя большинство программ считаются лицензионными, их «треснутые (crack)» версии с помощью различных методов широко используются на практике. Например, нелицензионная ОС Windows 10, антивирусные программные средства, офисные программные средства и др.

Технические средства защиты авторских прав. Используются разные методы защиты при обеспечении авторских прав. Они могут включать в себя такие процессы, как защита данных на CD/DVD дисках от несанкционированного копирования, а также ограничение возможности редактирования простых PDF-файлов. Вместе с тем, большинство людей думают, что, купив лицензионный CD диск, они также приобретают возможность его копирования.

Безопасность. Безопасное использование информации в Интернете становится предметом этических споров. В первую очередь это поднимает вопрос защиты общественного благосостояния или защиты прав личности. По мере увеличения числа пользователей Интернета растет и количество персональных данных, в результате увеличивается число киберпреступников.

Достоверность. Из-за наличия Интернета и характера некоторых людей или групп работа с достоверностью данных становится проблемой. Другими словами, кто несет ответственность за достоверность информации в Интернете? Кроме того, существует много споров о том, кто заполняет информацию в Интернете, кто должен нести ответственность за ошибки и недостатки в ней.

Доступность, цензура и фильтрация. Темы доступности, цензуры и фильтрации информации охватывают многие моральные вопросы, связанные с киберэтикой. Наличие этих проблем ставит под сомнение наше понимание конфиденциальности и частной жизни, а также наше участие в жизни общества. Предотвращение распространения этой информации на основе ограничения или фильтрации использования информации может повлиять на доступность. Цензура также может быть на низком уровне (например, компания для своих сотрудников) или на высоком уровне (осуществляемая правительством для обеспечения безопасности). Одним из лучших примеров управления, поступающими в страну данными, является проект «Великий Китайский Файрвол».

Свобода информации. Свобода информации, то есть свобода слова, а также свобода поиска, получения и передачи информации поднимают вопрос о том, кому и чему помогает при кибератаке. Право на свободу информации обычно зависит от ограничений, влияющих на общество или его культуру. Ограничения могут иметь различный вид. Например, в некоторых странах Интернет считается формой использования средств массовой информации, которой пользуются все резиденты страны. Кроме того, ограничения на использование Интернета могут различаться в разных штатах некоторых стран.

Цифровые барьеры. Кроме этических проблем, связанных со свободой информации, существует проблема, называемая *цифровым барьером*, которая представляет собой социальный

разрыв между людьми с ограниченным доступом к киберпространству. Этот разрыв между странами или регионами мира называется глобальным цифровым барьером.

Запрещенный контент (порнография). Использование несовершеннолетними запрещенного контента, доступного в Интернете, всегда было предметом этических дискуссий. Хотя использование такого контента строго запрещено в некоторых странах, а в некоторых странах оно разрешено.

Азартные игры. Эта проблема также является одной из дискуссий по вопросу этики, где одни люди считают это вредным, а другим не нравится вмешательство в них закона. Между сторонами, в свою очередь, вопросы – «Какие виды игр следует разрешить? Где они должны проходить?» вызывают широкую дискуссию. В настоящее время в большинстве стран этот вид игры легально разрешен, в то время как в остальных существуют строгие ограничения.

Этика использования компьютера. Институт этики использования компьютеров – некоммерческая организация, задачей которой является продвижение технологий с этической точки зрения. Со стороны этой организации перечислены следующие 10 этических правил:

- не используйте свой персональный компьютер в ущерб другим;
- не мешайте работе компьютера других пользователей;
- не смотрите на компьютерные файлы других пользователей;
- не используйте компьютер в целях кражи;
- не используйте компьютер в корыстных целях;
- не используйте и не копируйте программное обеспечение, которое вы не купили за свои собственные деньги;
- не используйте чужой компьютер без разрешения;
- не навредите чужим плодам интеллектуального труда;
- подумайте о социальных последствиях созданной вами программы;
- используйте свой компьютер сознательно и уважительно по отношению к другим.

Кодекс рационального использования информации. Кодекс рационального использования информации основан на пяти принципах, которые подчеркивают требования к системе бухгалтерского учета. Эти требования были введены

Министерством здравоохранения и социальных служб США в 1973 году:

- не должно быть систем сбора персональных данных;
- каждый должен уметь управлять тем, какая информация о нем хранится в системе и как его использовать;
- каждый должен иметь возможность контролировать использование собранной о нем информации по назначению;
- каждый должен корректировать информацию о себе;
- каждая организация, занимающаяся созданием, хранением, использованием или распространением набора персональных данных, должна гарантировать, что эта информация используется только по прямому назначению, и принять меры для предотвращения ее использования в других целях.

1.4. Безопасность человеческой деятельности

Социальная инжинерия – это совокупность различных психологических методов и практик мошенничества, целью которых является получение конфиденциальной информации о человеке посредством мошенничества. Конфиденциальная информация – имя пользователя/ пароли, личная информация, обвинительные доказательства, номера банковских карт и любая информация, которая может нанести финансовый или репутационный ущерб.

Данный термин происходит из области хакерства, *хакер* – человек, который ищет уязвимость в компьютерной системе, другими словами, «нарушитель». На данный момент хакеры прекрасно понимают, что главным слабым местом в любой системе является человек, а не машина. Человек, как и компьютер, работает по определенным законам. Используя опыт, накопленный человечеством в области психологии, уловок и механизмов воздействия, хакеры начинают «атаковать людей». Иногда их также называют «хакерами разума».

Например, предположим, что хакер хочет взять у вас деньги. Допустим, у него есть информация о вашем номере телефона и вашем аккаунте в социальной сети. Кроме того, в результате проведенных исследований он также выяснил, что у вас есть брат, и также собрал достаточно информации о вашем брате. Он также

знает номер телефона вашего брата. После этого он начал строить свой план на основе этой информации.

План: Хакер звонит вам вечером и представляется вашим братом (возможно, вместо вашего имени произносит «кличку», которым вас называет только ваш брат) и говорит, что наткнулся на хулиганов на улице и что они отняли все (телефон, деньги, пластиковую карту и т.д.). Кроме того, он говорит, что ему помогла девушка, и что у него с собой нет денег. При этом он утверждает, что у этой девушки с собой есть пластиковая карта, и требует вас перевести на эту пластиковую карту 20 000 сум, необходимой суммы, чтобы добраться до больницы. В 80% данных случаев хакеры добиваются успеха, и у опытного хакера выполнение этих работ не вызывает трудностей.

В этом случае можно говорить о возможности распознания голоса вашего брата. Однако человек может находиться в среде с разным возбуждением и шумом. Кроме того, если телефон зазвонил во время сна, вам становится все труднее определить голос.

Рассмотрим мышление, которое использует хакер в этом случае:

1. Хорошо замаскировался и основан на реальных примерах (например, ваши фотографии, места, о которых знают только ваши близкие и т.д.) и придумал хороший миф.

2. Все это сказано достаточно быстро и достоверно.

3. Был использован очень убедительный механизм воздействия – принуждение к жалости (обращение к эмоциям).

Угрозы, связанные с социальной инженерией, можно классифицировать следующим образом:

Угрозы, связанные с телефоном. Телефон по-прежнему является одним из наиболее распространенных способов связи внутри и между организациями. Поэтому он остается эффективным инструментом социальной инженерии. При разговоре по телефону невозможно подтвердить личность собеседника. Это позволяет злоумышленникам занимать положение сотрудника, начальника или любого, кто может доверять информации, которая кажется конфиденциальной или важной. В этом случае жертве ничего не остается, кроме как «помочь». Даже если запланированный разговор кажется незначительным.

Существуют различные методы мошенничества, направленные на хищение денег у пользователей мобильных телефонов. Сюда

могут входить звонки или выигрыши в лотерею, SMS-сообщения, запросы на возврат в случае ошибок или сообщения о том, что у близких родственников жертвы возникла проблема и им необходимо немедленно перевести определенную сумму денег.

В этих случаях требуются реализовать следующие меры безопасности:

- идентификация личности, звонившей по телефону;
- использование услуги идентификации номера;
- игнорирование неизвестных ссылок в SMS-сообщении.

Угрозы, связанные с электронной почтой. Многие сотрудники ежедневно получают десятки, даже сотни электронных писем от корпоративных и персональных почтовых систем. Конечно, невозможно уделить должное внимание каждой букве потока такой корреспонденции. Это значительно упрощает реализацию атак. Многие пользователи почтовых систем воспринимают такую ситуацию как электронный аналог переноса бумаг из одной папки в другую и сохраняют спокойствие при получении сообщений. Когда злоумышленник отправляет простой запрос по почте, его жертва часто делает то, что он просит, не задумываясь о его поведении. Электронные письма могут содержать гиперссылки, побуждающие сотрудников нарушать корпоративную среду защиты. Такие ссылки не всегда ссылаются на заявленные страницы.

Большинство мер безопасности разработаны для предотвращения использования корпоративных ресурсов неавторизованными пользователями. Пользователь, ссылаясь на гиперссылку, отправленной злоумышленником, позволяет обойти многие типы защиты, загрузив вредоносную программу в корпоративную сеть. Гиперссылка также может потребовать доступа к множеству хостов со всплывающими приложениями, которые требуют информации или помощи. Самый эффективный способ предотвратить мошенничество и вредоносные атаки – это смотреть на сообщения неожиданного пользователя с подозрением. Чтобы распространить этот подход по всей организации, необходимо ввести следующие элементы использования электронной почты, изложенные в политике безопасности:

- приложения к документам;
- гиперссылки в документе;
- запрашивать личную или корпоративную информацию внутри компании;

- запросы на личную или корпоративную информацию, поступающие из-за пределов компании.

Угрозы, основанные на использовании мгновенных сообщений. Обмен мгновенными сообщениями – уже завоевал популярность среди корпоративных пользователей. Благодаря скорости и простоте использования этот способ связи открывает широкий спектр возможностей для различных видов атак. Пользователи смотрят на него как на телефон и не рассматривают его как потенциальную программную угрозу. Существует два основных типа атак, основанных на использовании службы обмена мгновенными сообщениями – ссылка на вредоносную программу и отображение сообщения о самой программе. Одной из особенностей сервисов мгновенного обмена сообщениями является неформальность соединения, помимо возможности совпадения в нем любых имен, этот фактор позволяет злоумышленнику проявить себя как другое лицо. Это значительно повышает шансы на успешную атаку. Если компания хочет воспользоваться другими преимуществами для снижения затраты на получение мгновенных сообщений, она должна предусмотреть соответствующие механизмы защиты в своей корпоративной политике безопасности. Для надежного управления обменом мгновенными сообщениями в корпоративной среде необходимо выполнить следующие требования:

- выбрать единую платформу для обмена мгновенными сообщениями;
- определить параметры безопасности при настройке сервиса обмена мгновенными сообщениями;
- определить принципы установления новых отношений;
- установить стандарты выбора пароля;
- давать рекомендации по использованию мгновенных сообщений.

Специалисты по социальной инженерии рекомендуют следующие основные методы защиты организаций:

- разработка надежной политики классификации данных, учитывающей типы данных, которые кажутся безвредными, в форме важных данных;
- обеспечение безопасности данных клиентов с помощью шифрования данных или управления доступом;

- обучение сотрудников навыкам социальной инженерии, научить их скептически относиться к общению с незнакомыми людьми;

- запрет на обмен паролями или совместное использование между сотрудниками;

- запрет на передачу информации о предприятии лицу, которое лично не знакомо или не подтверждено каким-либо образом;

- использование специальных процедур аутентификации для тех, кто запрашивает использование конфиденциальной информации.

В большинстве случаев компании часто используют сложные многоуровневые системы безопасности для предотвращения атак социальной инженерии. Некоторые особенности и обязанности таких систем перечислены ниже:

- *физическая безопасность* – барьеры, ограничивающие использование помещений компании и корпоративных ресурсов. Не следует забывать, что ресурсы компании, например, мусорные контейнеры, расположенные за пределами территории компании, физически не защищены.

- *данные* – бизнес данные: счета, почта и др., при планировании анализа угроз и мер защиты данных необходимо определить принципы работы с бумажными, электронными носителями информации.

- *приложения* – программы, управляемые пользователями. Чтобы защитить свою среду, необходимо рассмотреть, как злоумышленники могут использовать почтовые программы, службы мгновенного обмена сообщениями и другие программы.

- *компьютеры* – установить строгие принципы, определяющие, какие программы можно использовать на корпоративных компьютерах, защитить компьютеры пользователей от прямых атак.

- *внутренняя сеть* – сеть, влияющая на корпоративные системы, может быть локальной, глобальной или беспроводной. Из-за популярности дистанционных методов работы в последние годы границы внутренних сетей были значительно расширены в произвольном порядке. Сотрудники компании должны понимать, что нужно делать при организации безопасной работы в любой сетевой среде.

- *периметр сети* – граница между внутренними сетями компании и внешними, например, Интернетом или сетями партнерских организаций.

Существует множество атак на социальную инженерию, ниже приведены некоторые из них:

Фишинг. Фишинг (англ. Phishing - рыбная ловля) – вид мошенничества в сети Интернет, целью которого является получение доступа к конфиденциальной информации пользователя (логин/пароль). В настоящее время это одна из наиболее распространенных схем социальной инженерии. Широкое распространение большого количества личной информации не может обойтись без «ветра» фишинга. В качестве наиболее распространенного примера фишинга можно указать поддельное сообщение от банка или платежной системы в виде официальной информации, отправленной на электронную почту жертвы. Такие электронные письма обычно содержат ссылку на поддельный веб-сайт в форме, аналогичной официальному веб-сайту, и требуют личной информации (рис. 1.5).

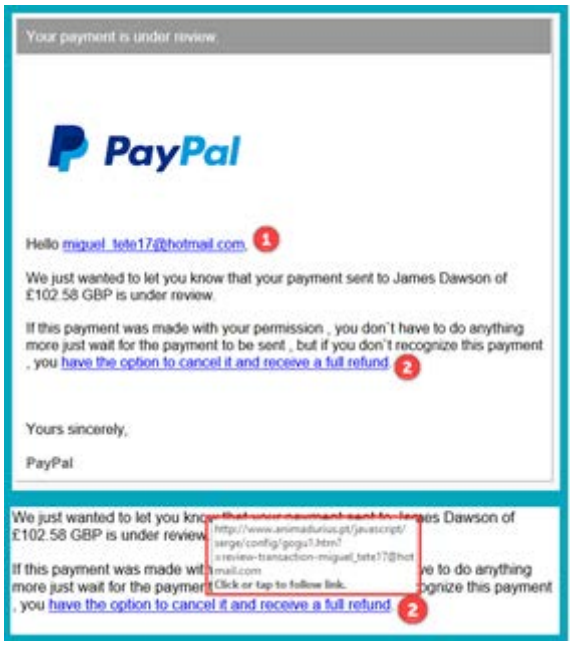


Рис.1.5. **Пример фишинг атаки**

В первом случае, показанном на рисунке, вместо имени и фамилии клиента или пользователя пишется почтовый адрес, во втором случае, когда мышь переносится по ссылке, можно увидеть другой адрес, а не фактический адрес (www.PayPal.com).

Ниже приведены примеры распространенных фишинговых схем.

Несуществующая ссылка. При этом типе фишинг-атаки рекомендуется ссылаться на веб-сайт, похожий на определенный веб-сайт. Например, адрес www.PayPai.com можно отправить как www.PayPal.com. В этом случае пользователи редко замечают, что буква «l» заменяется буквой «i». При переходе по ссылке веб-сайт похож на www.PayPal.com, но посещается поддельный веб-сайт и вводится запрошенная информация о платежной карте. В результате введенные данные попадают в руки хакера.

Ярким примером этого является фишинговое сообщение, которое распространилось среди пользователей eBay в 2003 году. В сообщении говорилось, что аккаунты пользователей были заблокированы и информация о кредитных картах должна быть разблокирована, а также содержалась ссылка на поддельный веб-сайт, похожий на официальный. Ущерб, нанесенный этой фишинг-атакой, составлял несколько сотен тысяч долларов.

Мошенничество, основанное на использовании известного корпоративного бренда. В этой форме мошенничества сообщение отправляется пользователю от имени известной или крупной компании. В сообщении могут быть поздравления с победой в конкурсе, проводимом компанией. В ней также запрашивается немедленно изменить данные учетной записи и пароля. Аналогичные схемы могут также осуществляться от имени службы технической поддержки.

Фальшивые лотереи. Согласно этой фишинговой схеме, пользователь может получить сообщение о том, что он является победителем лотереи, проводимой любой известной компанией. Со стороны это письмо выглядит так, как будто оно было отправлено от имени одного из высокопоставленных сотрудников компании.

Поддельные антивирусные и защитные программы. Эти программы называются мошенническим программным обеспечением или «шустрыми программами», и хотя они похожи на антивирусные программы, их функции отличаются. Это программное обеспечение пытается заманить пользователя в поддельные сделки на основе ложных уведомлений о различных угрозах. Когда пользователь их использует, он может сталкиваться с различными всплывающими окнами в электронной почте, онлайн-рекламе, социальных сетях, результатах поисковых систем

и даже на компьютере пользователя. В приведенном ниже примере представлен внешний вид поддельной антивирусной программы под названием Security Essentials 2010, которая на самом деле должна быть Microsoft Security Essentials (рис. 1.6).

IVR (Interactive Voice Response) или телефонный фишинг. Этот метод фишинговой схемы основан на использовании предварительно записанной системы обмена сообщениями для восстановления «официальных звонков» банка и других систем IVR. В этой атаке жертва связывается с банком и получает запрос на подтверждение или обновление какой-либо информации. Система требует подтверждения пользователя путем ввода ПИН-кода или пароля. В результате злоумышленник, получивший доступ к важным данным, сможет использовать данные пользователя. Например, нажмите «1», чтобы изменить пароль, и нажмите «2», чтобы получить ответ оператора и т.д.

Рис.1.6. **Антивирусная программа «Security Essentials 2010»**

Претекстинг. В этой фишинговой схеме хакер выдает себя за другое лицо и стремится получить конфиденциальную информацию по заранее подготовленному сценарию (скрипту). При этой атаке производится соответствующая подготовка, чтобы жертва не заподозрила: находятся такая информация, как дата рождения, ИНН, номер паспорта или последние цифры номера счета. Эта фишинговая схема обычно осуществляется по телефону или электронной почте.

Квид про кво (в латинице: Quid pro quo). Эта фраза в переводе с английского означает «услуга за услугу», и в этом типе социальной инженерии хакер обращается к компании через корпоративную сеть или электронную почту. Часто хакер представляется специалистом по техническому обслуживанию и говорит, что технический сотрудник «поможет» ему решить проблемы на рабочем месте. Во время «устранения» технической проблемы осуществляется внушение целевому лицу выполнение команд или установка различных программ на компьютер жертвы. Например, исследование, проведенное в рамках программы информационной безопасности в 2003 году, показало, что 90% офисных сотрудников были готовы предоставить конфиденциальную информацию, например, свои собственные пароли, за любую услугу или оплату.

Дорожное яблоко. В этом методе социальной инженерии хакер использует специальные вредоносные носители данных и оставляет их рядом с рабочим местом жертвы, в общественных и в других местах. При этом носители информации регистрируются в форме, соответствующей данной организации. Например, хакер оставляет диск с логотипом корпорации и адресом официального веб-сайта. Этот диск может называться «Заработная плата для руководителей». Жертва, получившая этот носитель, поместит его на свой компьютер и тем самым заразит его.

Сбор открытых данных. Техника социальной инженерии требует не только психологических знаний, но и умения собирать необходимую информацию о человеке. Относительно новым способом получения такой информации является сбор ее из открытых источников, социальных сетей. Например, такие сайты, как Одноклассники, ВКонтакте, Facebook, Instagram, содержат много информации, которую люди не пытаются скрыть. Часто пользователи, не уделяя должного внимания вопросам безопасности, оставляют без присмотра данные и сообщения, которые могут быть использованы хакером.

В качестве наглядного примера можно привести похищение сына Евгения Касперского. При этом выяснилось, что преступники знали повестку дня и маршрут подростка по публикациям на страницах социальных сетей.

Даже если вы ограничите доступ к информации на своей странице в социальной сети, нет полной гарантии, что пользователь не станет жертвой мошенничества. Например, бразильский

исследователь по компьютерной безопасности показал, что с помощью методов социальной инженерии можно подружиться с любым пользователем Facebook в течение 24 часов. В ходе эксперимента Нельсон Новаес Нето создает фальшивую учетную запись, изначально знакомого для жертвы – человека, например, его руководителя. Сначала Нето посылает запрос о дружбе друзьям руководителя жертвы, а затем непосредственно другу жертвы. Через 7,5 часов исследователь подружится с жертвой. В результате у исследователя появится возможность для извлечения личных данных пользователя.

Взгляд через плечо. Согласно этой атаке, злоумышленник получает информацию о жертве, оглядываясь через его плечо. Этот тип атак распространен в общественных местах, таких как кафе, автобусы, торговые центры, аэропорты и железнодорожные станции. Опросы, проведенные по этому нападению, показали следующее:

- 85% участников признались, что видели конфиденциальную информацию, которую им не нужно было знать;
- 82% участников признали, что их информация на экране может быть просмотрена посторонними лицами;
- 82% участников не верили, что сотрудники организации будут защищать свой экран от посторонних людей.

Обратная социальная инженерия. Тот факт, что жертва сама предоставляет информацию злоумышленнику, считается случаем обратной социальной инженерии. Хотя эта точка зрения на первый взгляд не имеет смысла, в большинстве случаев жертва сама прибегает к помощи злоумышленника для решения своих проблем. Например, злоумышленник, работающий с жертвой, может переименовать файл на компьютере жертвы или скопировать его в другой каталог. Жертва, зная, что файл отсутствует, захочет, как можно скорее устранить проблему. В этой ситуации злоумышленник представляет себя специалистом по устранению неполадок и, помимо решения проблемы жертвы, также получает принадлежащий ему логин / пароль. Кроме того, с помощью этой задачи злоумышленник будет иметь репутацию внутри организации и добьется увеличения числа своих жертв. Определение этой ситуации является достаточно сложной задачей.

Известные социальные инженеры. Кевин Митник – один из самых известных социальных инженеров в истории, всемирно

известный компьютерный хакер, эксперт по безопасности, а также автор множества книг по компьютерной безопасности, основанных на социальной инженерии. По его мнению, получить пароль обманным путем легче, чем взломать систему безопасности.

Братья Бадир. Несмотря на то, что братья Бадир, Мушид и Шади Бадир, были слепыми от рождения, они сумели реализовать несколько крупных схем мошенничества в Израиле в 1990-х годах, использовав социальную инженерию и подделку голоса. В телеинтервью они сказали: «Полностью от сетевых атак застрахован лишь тот, кто не пользуется телефоном, электричеством и ноутбуком».

Способы защиты от социальной инженерии. Для проведения своих атак злоумышленники, применяющие техники социальной инженерии, зачастую эксплуатируют доверчивость, лень, любезность и даже энтузиазм пользователей и сотрудников организаций. Защититься от таких атак непросто, поскольку их жертвы могут не подозревать, что их обманули.

Атаки социальной инженерии можно определить следующим образом:

- представление себя другом либо новым сотрудником с просьбой о помощи;
- представление себя сотрудником поставщика, партнерской компании, представителем закона;
- представление себя кем-либо из руководства;
- представление себя поставщиком или производителем, который устраняет уязвимость или предоставляет жертве возможность что-то обновить;
- предложение помощи в случае возникновения проблемы;
- использование внутреннего спокойствия и терминологии для возникновения доверия;
- отправка различных вредоносных программ в качестве приложения к «письму»;
- использование фальшивого окна, с просьбой ввести логин/пароль повторно;
- предложение приза за регистрацию на сайте с именем пользователя и паролем;
- записывание клавиш, которые жертва вводит на своём компьютере или в своей программе (кейлоггинг);

- подбрасывание различных носителей данных с вредоносной программой на стол пользователя;
- голосовые сообщения о различных звонках и т.д.

Проблемы, связанные с социальной инженерией, можно увидеть во многих аспектах жизни. В частности, использование социальной инженерии широко распространено в массовой культуре (например, в кинофильмах). Например, следующие фильмы содержат эпизоды социальной инженерии:

- «Поймай меня, если сможешь»;
- «Поймай толстуху, если сможешь»;
- «Один дома»;
- «Хакеры»;
- «Афера Томаса Крауна»;
- «Бриллианты навсегда»;
- «Кто я».

Контрольные вопросы

1. Жизненные образы информационной безопасности и их функции.
2. Дайте объяснение понятию кибербезопасности.
3. Какова структура кибербезопасности как науки?
4. Основные понятия кибербезопасности.
5. Что вы понимаете под обеспечением конфиденциальности информации?
6. Что вы понимаете под обеспечением целостности информации?
7. Важность доступности информации.
8. Риск и его роль в кибербезопасности.
9. Почему нужно думать, как злоумышленник?
10. Что такое системное мышление и почему оно необходимо?
11. В чем разница между понятиями информационной безопасности и защиты информации?
12. Что такое актив?
13. Дайте объяснение понятиям угроза и уязвимость.
14. В чем разница между понятиями информационной безопасности и кибербезопасности?

15. Каковы области знаний о кибербезопасности, и каковы их основные характеристики?
16. Объясните человеческий фактор в кибербезопасности на примерах.
17. Дайте объяснение понятию киберпреступность.
18. Цели осуществления киберпреступности.
19. Основные виды киберпреступности.
20. Дайте объяснение понятию киберэтика и приведите примеры.
21. На какие этические правила необходимо обращать внимание при использовании компьютера?
22. Дайте информацию о способах предотвращения киберпреступности и законы о киберпреступности.
23. Что говорится в Законе «О принципах и гарантиях свободы информации» о порядке использования информации?
24. Какие пункты о киберпреступности содержит Кодекс Республики Узбекистан «Об административной ответственности»?
25. Какие пункты о киберпреступности содержит Уголовный кодекс Республики Узбекистан?

ГЛАВА 2. АРХИТЕКТУРА, СТРАТЕГИЯ И ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ

2.1. Архитектура и стратегия кибербезопасности

В условиях современной коммерции комплекс сложных вопросов ещё больше повысит их актуальность в условиях нестабильной экономической ситуации. К таким вопросам можно включить следующее:

- увеличение дохода;
- увеличение скорости реакции на меняющиеся ситуации;
- снижение расходов и затрат;
- ускорение инноваций;
- сокращение сроков предоставления товаров и услуг на рынок;
- повышение объективности заказчиков и партнеров;
- повышение конкурентоспособности;
- обеспечение соответствия нормативным требованиям.

Для решения всех вышеперечисленных вопросов используется архитектура предприятия (рис.2.1). Архитектура предприятия позволяет сформировать набор принципов, подходов и технологий, определяющих основу для его дальнейшей трансформации, роста и развития с учетом текущего состояния организации.

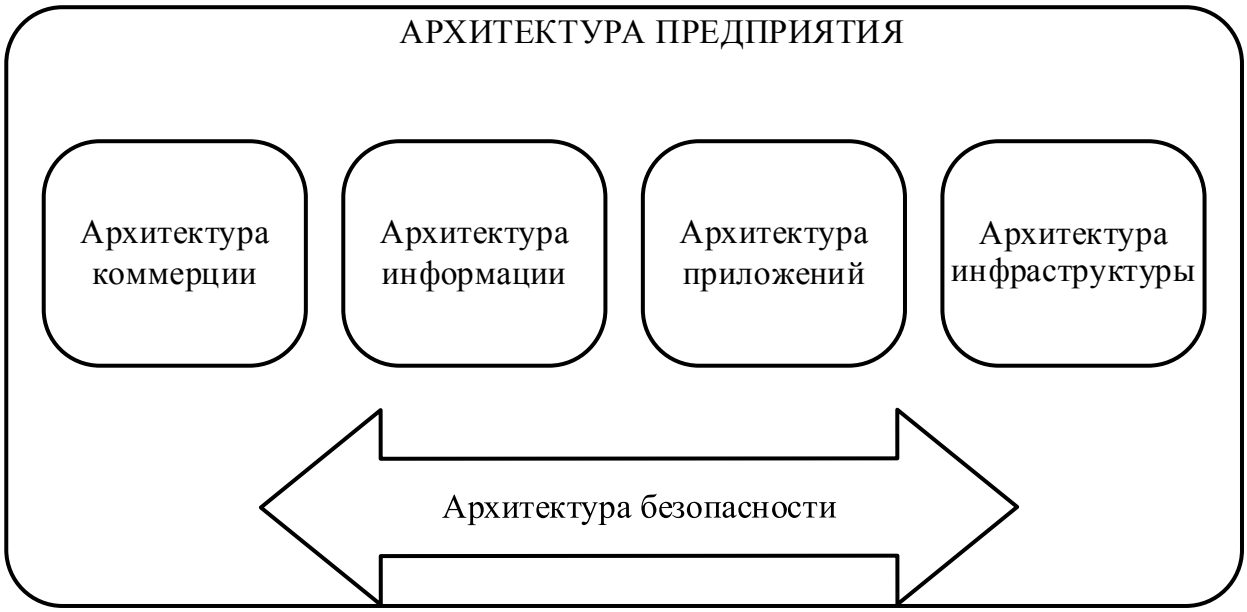


Рис.2.1. **Архитектура предприятия и её взаимосвязь с другими архитектурами**

В настоящее время существует несколько подходов к созданию таких архитектур, например, TOGAF, Zachman Framework, FEAF, DoDAF и др.

Однако какой бы подход ни был выбран, в современных условиях невозможно развиваться без использования информации и информационной системы. Информация и информационные системы не только поддерживают любые изменения в коммерции, но и делают их предсказуемыми, подготавливают их заранее, в ряде случаев способствуют появлению новых коммерческих возможностей. Однако коммерция не всегда развивается так, как хотелось бы. Информационно-операционные риски, связанные с утечкой данных, выхода из строя элементов информационно-технологической инфраструктуры и т.д. играют важную роль в этом. Архитектура информационной безопасности, которая неразрывно связана с другими архитектурами предприятия, необходима для подготовки к текущим и будущим рискам.

Архитектура кибербезопасности описывает процессы, человеческие роли, технологии и разнообразную информацию и учитывает сложность и изменчивость современного предприятия. Другими словами, архитектура кибербезопасности описывает состояние любой системы информационной безопасности организации и связанных с ней компонентов и интерфейсов. При этом архитектура информационной безопасности отражает текущие и, главное, будущие потребности коммерции.

Обычно выделяют 3 уровня архитектуры – концептуальный, логический и реализационный (технологический). На рис. 2.2 показана такая архитектура, технологическая часть которой, обычно находится вне контроля службы безопасности.

Как перейти от текущего состояния к новому, более совершенному и более соответствующему поставленным целям состоянию? Для этого есть стратегия, то есть направление действий для достижения поставленных целей.

Стратегия – комплекс структурированных и взаимосвязанных действий, призванных обеспечить непрерывную успешную работу предприятия. На рис. 2.3 показана взаимосвязь между архитектурой и стратегией. Стратегия определяет оптимальный способ ее достижения, имея цель в виде архитектуры кибербезопасности.

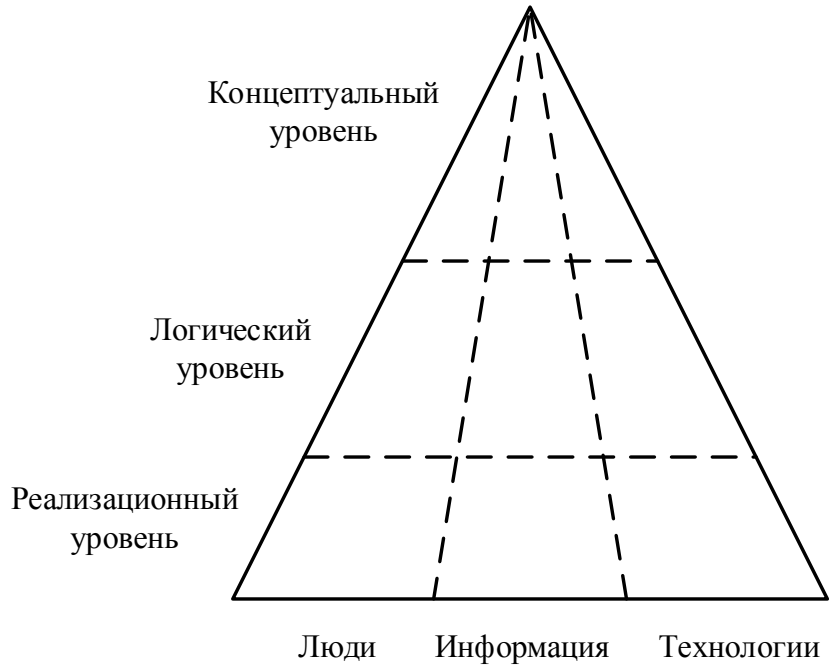


Рис.2.2. **Архитектура кибербезопасности**

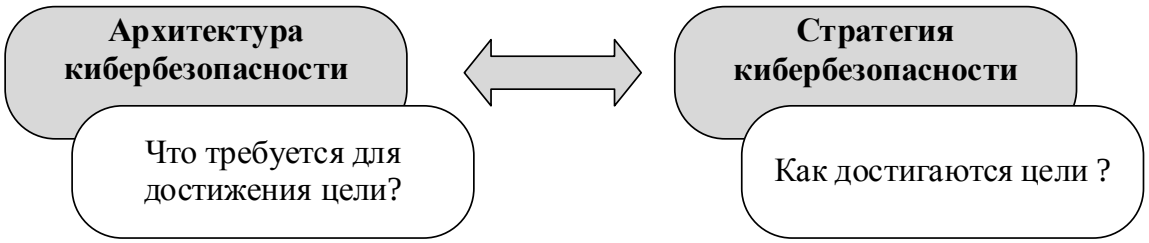


Рис.2.3. **Взаимосвязь между архитектурой и стратегией**

Часто разрабатывается стратегия кибербезопасности, которая включает архитектурное описание без различия между стратегией и архитектурными концепциями. Это не совсем правильно, потому что архитектура, то есть цели, могут не меняться со временем, в то время как стратегия достижения этих целей может серьезно меняться в зависимости от внешних и внутренних факторов. Если стратегия и архитектура описаны в одном документе, архитектура должна измениться по мере изменения стратегии.

2.2. Политика кибербезопасности и её реализация

Политика информационной безопасности (или политика безопасности) – план высокого уровня, описывающий цели и задачи организации, а также меры обеспечения безопасности.

Политика описывает безопасность в обобщенных терминах. Она планирует все программы по обеспечению безопасности. Политика информационной безопасности должна обеспечивать защиту процессов решения организационных вопросов или защиту рабочих процессов.

Аппаратные средства и программное обеспечение являются инструментами, обеспечивающими рабочий процесс, и они должны быть охвачены политикой безопасности. Поэтому в качестве основной задачи необходимо рассматривать полную инвентаризацию системы (включая сетевую карту). При составлении сетевой карты необходимо определить информационный поток в каждой системе. Схема информационных потоков может показать, в какой степени информационные потоки обеспечивают бизнес-процессы, а также отрасли, в которых важно принимать дополнительные меры для обеспечения защиты и жизнеспособности информации. Кроме того, с помощью этой схемы можно определить место, где обрабатывается информация, как эта информация должна храниться, записываться, перемещаться и контролироваться.

Инвентаризация помимо аппаратного и программного обеспечения должна охватывать такие ресурсы как, программно-аппаратная документация, технологическая документация и т.д., не связанные с компьютером. В составе этих документов могут быть сведения об особенностях организации коммерции, и эти документы указывают места, которые злоумышленники могут использовать.

Необходимость политики безопасности:

- увеличение количества устройств, используемых в организации, приводит к увеличению количества информации, передаваемой и хранимой в сети. эта ситуация, в свою очередь, также приводит к увеличению угроз безопасности, возникших в результате различных уязвимостей. политика безопасности позволяет организации бороться с этими угрозами и защищать ее от потери информации.

- политика безопасности обеспечивает соблюдение согласованных задач принципов безопасности за счет безопасного выполнения всех функций организации. политика безопасности обеспечивает соблюдение стандартов информационной безопасности при построении доверительных отношений с

клиентами. политика безопасности помогает снизить риск подтверждения компании внешним информационным угрозам.

- политика безопасности обеспечивает правовую защиту, определяя, какие правила должны использоваться в сети, как хранится конфиденциальная информация и какие алгоритмы шифрования необходимы для уменьшения раскрытия информации и уменьшения ответственности организации.

- политика безопасности снижает вероятность нарушений безопасности за счет прогнозирования угроз до их возникновения и выявления уязвимостей.

- она также сводит к минимуму риск потери и утечки данных организации за счет внедрения методов резервного копирования и восстановления.

Преимущества политики безопасности:

- *повышенная безопасность данных и сети:* организации осуществляют политику, основанную на сети, обеспечивающие безопасность своих данных. политика безопасности обеспечивает защиту при передаче данных из других систем в сети.

- *снижение рисков:* за счет реализации политики безопасности снижаются возможные риски от внешних источников. если сотрудники действуют на основе политики безопасности, то случаев потери данных и ресурсов практически не наблюдается.

- *мониторинг и контроль использования устройств и трансфера данных:* поскольку политика безопасности осуществляется сотрудниками, необходимо, чтобы администраторы постоянно контролировали трафик в организации и используемые внешние устройства. входящий и исходящий трафик должен отслеживаться и проверяться на регулярной основе.

- *высокая производительность сети:* перегрузки не будут доступны, если политика безопасности реализована правильно и сеть постоянно контролируется. скорость передачи данных в сети увеличится, и это приведет к увеличению общей эффективности.

- *моментальное реагирование на проблемы и отсутствие времени бездействия:* реализация политики безопасности дает возможность немедленно реагировать при обнаружении сетевых проблем.

- *снижение уровня волнения в управлении:* при реализации политики безопасности менеджер будет меньше волноваться. задача в политике безопасности обязательно должна быть

прикреплена к определенному сотруднику организации. если такая ситуация будет реализована, то в управлении не возникнет беспокойства, даже если в сети будет обнаружена неисправность.

- *снижение затрат:* если сотрудники будут следовать политике должным образом, избыточные затраты на различные препятствия, влияющие на организацию, будут уменьшены.

Иерархия политики безопасности:

При разработке политик безопасности в организациях используются различные документы. Разработка этих документов зависит от уровня иерархии политики безопасности и ее количества.

- *законы.* Законы расположены на самом верхнем уровне иерархии и включают в себя задачи, которые должен выполнять каждый сотрудник в организации. для каждого сотрудника, который не соблюдает эти законы, должны быть приняты меры ответственности.

- *нормативные документы.* Нормативные акты являются второй составляющей в иерархии, которые гарантируют соблюдение работниками законов. нормативный документ – совокупность руководящих документов, соответствующая закону о политике безопасности и состоящая из государственных или социальных нормативных документов.

- *политики.* С помощью политик организация создаёт законные внутренние сетевые требования для обеспечения безопасности персональных сетей. политика состоит из различных процедур, отражающих архитектуру безопасности организации. реализация этих политик позволит организации выполнять такие задачи, как установление стандартов и управление рисками.

- *стандарты.* Стандарты описывают методы реализации политики и осуществляются организациями. стандарты являются добровольными и обязательными в соответствии с политикой предприятия, и не должны требовать изменения по истечении определённого периода времени. стандарты также включают средства контроля безопасности, в зависимости от технологии, устройства и программного обеспечения.

- *инструкции.* Инструкции помогают организации противостоять угрозам, определяя стратегии реализации политик и стандартов организации. поэтому сотрудники организации проходят специальное обучение, чтобы выполнять инструкции.

- *процедуры.* Процедуры – набор последовательных шагов в реализации политики организации, для реализации которых требуется одобрение привилегированного субъекта. процедуры работают на основе следующих вопросов:

- кто что выполняет?;
- какие у них этапы?;
- какие формы и документы они используют?.

- *общие правила.* Общие правила – документ, обеспечивающий рекомендациями по выбору, использующийся в отсутствии каких-либо специальных стандартов. общие правила выглядят как рекомендации, и организации не смогут от них отказаться. хотя выполнение общих правил снижает риски, рекомендуется также изменять общие правила при изменении бизнес-требований.

Политика безопасности должна обладать следующими характеристиками:

- *краткость и ясность:* политика безопасности должна быть краткой и ясной при реализации в инфраструктуре. сложные политики безопасности трудны для понимания и не могут быть реализованы так, как ожидают сотрудники.

- *доступность:* политика должна быть простой в написании и спроектированной для различных секторов организации. хорошо написанная политика будет легко управляться и реализовываться.

- *экономическая обоснованность:* организации должны проводить экономичную и повышающую собственную безопасность политики.

- *практичность:* политика должна быть практичной, основанной на реальность. реализация нереальной политики создаст проблему для организации.

- *устойчивость:* организация должна иметь устойчивость в реализации своей политики.

- *процедурная терпимость:* когда выполняются политические процедуры, они должны соответствовать работодателю и работнику.

- *соответствие кибер и юридическим законам, стандартам, правилам и инструкциям:* осуществляемая добровольная политика должна соответствовать правилам и руководствам, разработанным на основе киберзаконов.

Типы политик информационной безопасности. Политика считается важной при планировании, разработке и внедрении информационной безопасности в организации, и она предоставляет пользователям решения существующих проблем в достижении целей безопасности. Кроме того, политика безопасности описывает функции программного обеспечения и оборудования в организации.

На предприятиях в сфере информационных технологий применяются следующие политики безопасности:

- *политика информационной безопасности организации (Enterprise Information Security Policies, EISP):* этот тип политики поддерживает безопасную среду организации, предлагая ей идеи, цели и методы. Она определяет методы разработки, реализации и управления программами безопасности. Кроме того, данная политика гарантирует соблюдение требований предлагаемой и запрашиваемой структуры информационной безопасности.

- *политики безопасности, ориентированные на проблемы (Issue-Specific Security Policies, ISSP):* эти политики ориентированы именно на проблемы с безопасностью в организации, а охват и сфера применения этих политик безопасности будет зависеть от типа проблемы и используемых в ней методов. В ней показаны профилактические меры, например, необходимые технологии для авторизации прав доступа пользователей.

- *политики безопасности, ориентированные на систему (System-Specific Security Policies, SSSP):* реализация этой политики безопасности включает в себя обеспечение общей безопасности определённой системы в организации. При этом организации в целях поддержки системы разрабатывают и управляют политиками SSSP, которые включают процедуры и стандарты. Кроме того, технологии, используемые организацией, включают в себя политику, направленную на систему. Эта политика может учитывать реализацию, конфигурацию и действия пользователей технологии.

В организациях может существовать множество политик безопасности, направленных на различные цели. Ниже приведены некоторые из них.

Политика использования Интернета. Настоящая политика определяет ограничения на использование Интернета и устанавливает порядок использования Интернета сотрудниками.

Политика использования Интернета включает в себя разрешения на доступ в Интернет, безопасность системы, установку сети, услугу ИТ и охватывает другие инструкции.

Политику использования Интернета можно разделить на следующие четыре категории:

1. *Беспорядочная политика (Promiscuous Policy):* эта политика не имеет ограничений на использование системных ресурсов. Например, согласно этой политике, пользователь может получить доступ к любому сайту, загрузить любое приложение, использовать удалённый компьютер или сеть. Хотя эта политика может быть полезной для сотрудников, работающих в офисах корпоративных организаций, или посетителей организации, она может сделать компьютер уязвимым для угроз, основанных на вредоносных программах. То есть, поскольку ограничений на использование Интернета нет, вредоносные программы могут проникать в результате незнания пользователей.

2. *Политика, основанная на разрешениях (Permissive Policy):* согласно этой политике блокируются только опасные услуги/ атаки и поведение. Например, в разрешающей политике Интернета основная часть Интернет-трафика будет открыта, за исключением ряда распространённых вредоносных служб/ атак. Только благодаря широко распространённым атакам и блокировке вредоносных программ администратор может обеспечить защиту от вредоносных действий в текущем состоянии. Эта политика всегда требует обнаружения новых атак и вредоносных программ и внесения их в базу данных.

3. *Параноидальная политика (Paranoid Policy):* согласно параноидальной политике, все будет заблокировано и будут введены строгие ограничения на компьютеры организации, использующие систему или сеть. В соответствии с настоящей политикой пользователь может вообще не быть подключён к Интернету или может быть подключён со строгими ограничениями. В таких случаях пользователи обычно пытаются обойти правила политики.

4. *Разумная политика (Prudent Policy):* Разумная политика реализуется после блокировки всех служб, при этом безопасные и необходимые службы разрешаются администратором индивидуально. Она регистрирует все события, связанные с

системной/ сетевой активностью, обеспечивая максимальную безопасность.

5. *Политика оптимального использования.* Политика оптимального использования состоит из правил, установленных владельцами сети и веб-сайтов, и определяет правильное использование вычислительных ресурсов. Эта политика устанавливает обязательство пользователей защищать информацию, содержащуюся в их аккаунтах, и требует от пользователя принятия ограничений политики при использовании сети или компьютера в Интернете. Разумная политика включает в себя принципы, запреты, пересмотр и меры наказания, которые запрещают пользователю использовать корпоративные ресурсы в личных целях.

Политика оптимального использования является неотъемлемой частью политики информационной безопасности. При этом организации получают гарантийное письмо о том, что новые сотрудники ознакомлены с политикой оптимального использования, прежде чем разрешать им использовать информационные ресурсы. Политика оптимального использования охватывает ключевые аспекты того, что пользователи должны и не должны делать в инфраструктуре информационных технологий.

Администратор должен проводить регулярные аудиты безопасности, чтобы гарантировать правильную реализацию политики оптимального использования. Например, большинство организаций запрещают вести переговоры на политические и религиозные темы на своих сайтах и по почте. В большинстве политик оптимального использования за нарушение налагаются наказания. Такие наказания могут варьироваться от временного закрытия аккаунта пользователя до законных наказаний.

Контрольные вопросы

1. Сущность архитектуры и уровней информационной безопасности.
2. Понятие стратегии информационной безопасности.
3. Роль стратегии и архитектуры безопасности в построении архитектуры предприятия.

4. Политика информационной безопасности и ее основная функция.
5. Почему необходима политика безопасности?
6. Состав и структура политики безопасности.
7. Основные типы политики безопасности.
8. Политика использования Интернета.

ГЛАВА 3. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

3.1. Основные понятия криптографии

Вопрос передачи важной информации определенному адресату, в тайне от других, может быть решен тремя способами:

- за счет создания абсолютно надежного скрытого канала передачи информации между адресатами. Однако в реальных условиях сделать это сложно;
- за счет сокрытия факта передачи путем маскировки канала передачи или трафика;
- за счет изменения информации таким образом, чтобы ее мог восстановить только законный получатель.

Именно третий вариант является предметом изучения криптографии. В настоящее время, вопросам, решаемым в рамках криптографии, относятся:

- обеспечение конфиденциальности информации;
- обеспечение целостности информации;
- реализация методов аутентификации;
- обеспечение неотказуемости в действии.

Свойство конфиденциальности обеспечивается за счет криптосистем с симметричным и открытым (асимметричным) ключом. Свойство целостности осуществляется с использованием криптографических хеш-функций и цифровых подписей. Системная часть аутентификации может реализоваться на основе криптографических примитивов (cryptographic primitives). Свойство действия описывает, как получатель сообщения защищен от попытки отправителя отрицать авторство ранее отправленного сообщения. Данное свойство обеспечивается только с помощью криптографических средств с открытым ключом.

Вышеупомянутые вопросы криптографии реализуются с использованием ряда криптографических примитивов:

- симметричные криптосистемы;
- криптосистемы с открытым ключом;
- криптографические хеш-функции;
- цифровые подписи;

- цифровые сертификаты.

Ниже приводится разъяснение основных терминов, используемых в последующих утверждениях.

Алфавит – конечный набор информации, используемый для представления информации. В современных криптосистемах часто используется двоичный алфавит, состоящий только из двух символов (0, 1). Также можно привести в качестве примера алфавит узбекского языка, состоящий из тридцати шести знаков (букв), русский алфавит, состоящий из тридцати двух знаков (букв), латинский алфавит, состоящий из двадцати восьми знаков (букв), алфавит компьютерных символов ASCII, состоящий из двухсот пятидесяти шести знаков (букв).

Текст или сообщение – набор отсортированных по алфавиту элементов. *Открытый текст* (plaintext) – исходное сообщение, предназначенное для шифрования. *Зашифрованный текст* (cipher text) – результат шифрования открытого текста.

Шифрование (encryption, enciphering) – процесс преобразования открытого текста в зашифрованный текст.

Расшифровка (decryption, deciphering) – обратный процесс, преобразующий зашифрованный текст в открытый текст.

Дешифрование (breaking) – процесс восстановления открытого текста на зашифрованном тексте, без знания ключа.

Сосредоточимся на разнице между расшифровкой и дешифровкой: если расшифровка считается стандартным состоянием обработки при использовании криптографического алгоритма, то дешифровка, скорее всего, для криптоанализа, является нарушением криптосистемы. Общий термин «шифрование» означает процесс шифрования и расшифровки.

Методы взлома криптосистем являются предметом изучения *криптоанализа*. Поскольку криптография и криптоанализ тесно связаны, их часто рассматривают в совокупности как единую науку – криптологию (kryptos - скрытая, logos - наука).

Криптосистема (cryptosystem) – семейство обратимых преобразований открытого текста в шифртекст, каждое из которых определяется соответствующим алгоритмом и значением ключа.

Ключ (key) или криптопеременная (cryptovariable) – конкретное значение некоторых параметров криптографического алгоритма, обеспечивающее выбор одного преобразования из семейств.

Внешний вид криптосистемы в виде «черного ящика» представлен на рис. 3.1.

Рис.3.1. **Вид криптосистемы в виде «черного ящика»**

Рассматривая криптосистему как систему с двумя составляющими: алгоритмом и ключом следует упомянуть *принцип Керкгоффа*. Согласно этому принципу, в секрете должен храниться только ключ, а алгоритм шифрования должен быть открытым. Это означает, что система не будет дискредитирована, даже если злоумышленник знает алгоритм. А ключ можно заменить. Клод Шеннон описал этот принцип как «Враг знает систему».

В большинстве случаев пользователи понимают понятия *шифрования* и *кодирования* данных как одно и то же. *Кодирование* – преобразование данных в другой формат, используя схему, открытую для всех (даже для злоумышленника), чтобы легко восстановить данные в исходное состояние. Кодирование осуществляется для обеспечения удобства использования информации и использует схемы, открытые для всех.

В процессе *шифрования* информация также преобразуется в другой формат. Однако, только определенные лица (лица, имеющие ключи расшифровки) смогут повторно преобразовать их. Основной целью шифрования является обеспечение конфиденциальности информации, и ее повторное преобразование ограничено некоторым лицам (тем, у кого не имеются ключи расшифровки).

Поскольку криптография и *стеганография* имеют сходство в областях науки, в большинстве случаев их путают. *Стеганография* – сокрытие конфиденциальной информации в открытых информационных массивах. Другими словами, основная идея стеганографии – избежать подозрений в существовании конфиденциальной информации.

В *криптографии* отправитель перед передачей сообщения по открытой сети (например, Интернет) преобразует сообщение в

зашифрованный текст. Когда это зашифрованное сообщение поступает к получателю, оно снова возвращается в режим обычного текста. В общем, *основная цель шифрования данных* (на основе симметричных криптографических систем или систем с открытым ключом - неважно) – сохранить конфиденциальность данных в тайне от остальных.

История криптографии. Самые ранние формы шифрования данных использовались тысячи лет назад. Шифры, которые использовались до последних десятилетий, назывались *классическими* шифрами. Развитие криптографии как науки изучалось в большинстве литературных источников на основе разных подходов, разделенных на несколько периодов. Например, в некоторых источниках шифры, использованные до создания вычислительных устройств, относятся к периоду *классических шифров*. А последующий период называют периодом современной криптографии. Однако, поскольку период до создания вычислительных устройств был очень долгим, важно было разделить их на части. Поэтому становление криптологии как науки можно условно разделить на следующие периоды:

1. *Древний период (классические шифры древнего периода).* Классические шифры этого периода в основном основаны на транспозиции алфавитной замены и замены мест. Например, методы квадрата Цезаря, Полибия.

2. *Средний период (классические шифры среднего периода).* В этот период шифры в основном базировались на многоалфавитной подстановке, и в качестве примера можно привести методы Вижинера, Атбаша. Шифры этого периода имели более высокую устойчивость, чем шифры первого периода.

3. *Период 1 и 2 – мировых воин (классические шифры периода 1 и 2 мировой войны).* Криптосистемы этого периода были в основном основаны на электромеханике, в которой осуществлялась передача зашифрованного текста (кода Морзе) с помощью радиоволн. В качестве примеров методов шифрования для этого периода можно привести телеграмму Zimmermann, шифр Энигма, машины SIGABA.

4. *Период компьютера (современные шифры).* Шифры этого периода предназначены для вычислительных устройств и обладают высоким уровнем безопасности. В качестве примера современных

шифров можно привести (все симметричные) DES, AES, ГОСТ 28147-89, IDEA, A5/1, RC4 и (с открытым ключом) RSA, Эл-Гамал.

Основные разделы криптографии. Криптографию можно разделить на следующие разделы:

1. *Криптография с симметричным ключом.* Общий вид криптографии с симметричным ключом показан на рис. 3.1, на котором при шифровании и расшифровании используется один (симметричный) ключ. Криптосистемы с симметричным ключом также называют криптосистемами с *одним ключом*. Это означает, что для использования алгоритмов шифрования с симметричным ключом необходимо, чтобы обе стороны имели один и тот же ключ. Симметричный ключ обычно генерируется на одной стороне и безопасно доставляется на другую сторону с использованием специальных методов.

2. *Криптография с открытым ключом.* В криптографии с открытым ключом (также называемой асимметричной криптографией), если шифрование данных выполняется с помощью *открытого ключа* получателя, их расшифровка выполняется с помощью *закрытого ключа* получателя. Поэтому криптосистемы с открытым ключом также называют криптосистемы с двумя ключами. Общий вид криптографии с открытым ключом представлен на рис. 3.2.

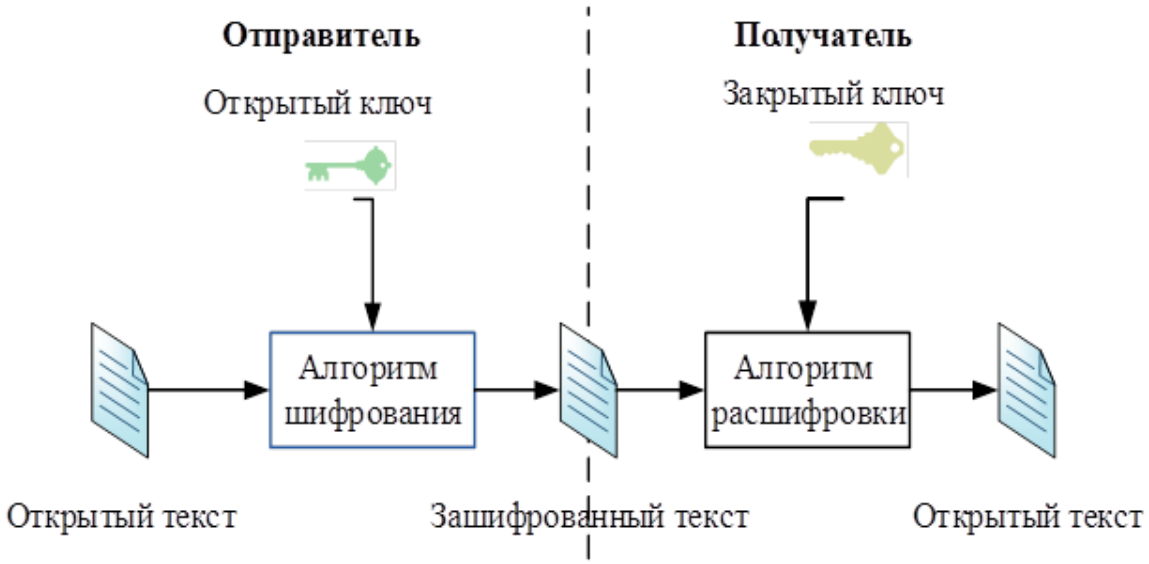


Рис.3.2. **Общий вид шифрования с открытым ключом**

Для обмена информацией на основе криптографических алгоритмов с открытым ключом отправитель должен сначала иметь

открытый ключ получателя. Открытый ключ получателя используется только для шифрования данных, и расшифровать шифр с его помощью невозможно. Точно также нет возможности зашифровать данные с помощью закрытого ключа. Расшифровка зашифрованного текста допустимо только для владельца закрытого ключа. Следовательно, закрытый ключ должен храниться в безопасности владельцем и не должен быть известен никому, кроме него самого.

3. *Хеш-функции.* Шифрование данных осуществляется для того, чтобы гарантировать их целостность, и если данные изменятся во время передачи, это можно будет обнаружить. В хэш-функциях обычно длина входящих данных является переменной, в то время как на выходе она возвращает значение переменной длины. В качестве современного примера хэш-функциям можно привести MD5, SHA1, SHA256, O‘z DSt 1106:2009.

Обычно в криптографии при шифровании (расшифровке) информации используется два типа *отражения*. Один из них – *отражение подстановки (substitution)*, другой – отражение перестановки *(permutation).*

Отражение подстановки. Это отражение лежит в основе простых и современных симметричных криптографических алгоритмов. В отражении подстановки символы открытого текста берутся из одного алфавита, а соответствующие символы зашифрованного текста берутся из другого алфавита.

Ниже приводится текст, полученный для шифрования на основе простой операции отражения перестановки. Этот простой метод шифрования известен под именем Цезарь. Например, если открытый текст равен «HELLO», то в соответствии с ним зашифрованный текст будет равен «KHOOR». В этом случае алфавит зашифрованного текста формируется путем перемещения алфавита открытого текста на 3 позиции, и поэтому ключ шифрования можно рассматривать как 3 (табл.3.1). В процессе расшифровки символы шифр текста извлекаются из алфавита шифр текста, заменяя их символами соответствующего открытого текстового алфавита. Например, если зашифрованный текст равен «ILUVW», то соответствующий открытый текст будет равен «FIRST».

Таблица 3.1

Пример на отражение подстановки

Открытый текст	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Зашифрованный текст	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Отражение перестановки. Согласно этому отражению, положение символов открытого текста меняется в соответствии с определённым правилом. В этом случае символы, присутствующие в открытом тексте, также присутствуют в шифре, только их места меняются местами (рис. 3.3).

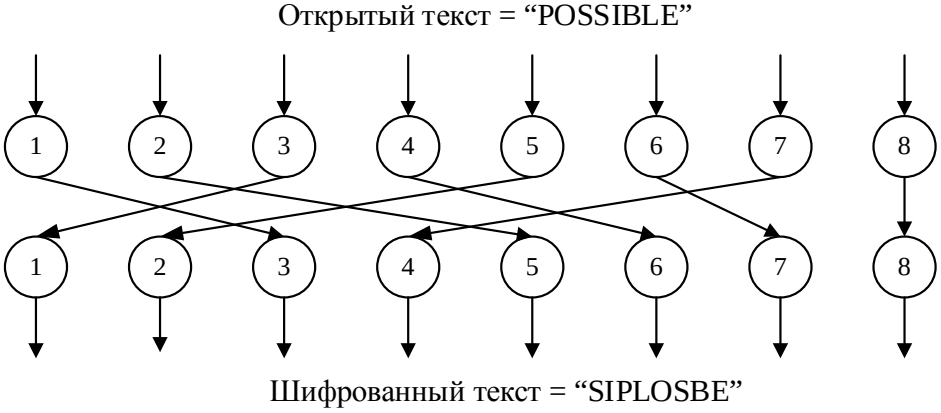


Рис.3.3. **Пример простого метода перестановки**

Одноразовый блокнот. Криптосистема, известная как одноразовый блокнот или «шифр Вернама», представляет собой *надежный* алгоритм шифрования, который широко использовался на протяжении всей истории. Основная причина, по которой он называется одноразовым, заключается в том, что *ключ (блокнот)* в нем используется только один раз, что в большинстве случаев реализация его невозможна. Например, допустим, что этот алгоритм шифрования представляет собой алфавит из 8 символов.

Полученные двоичные значения представлены в табл. 3.2. Символы алфавита и соответствующие им битовые значения открыты для всех и не являются секретными.

Таблица 3.2

Алфавит, выбранный для открытого текста

Символы	B	E	I	L	O	P	S	T
Бинарное значение	000	001	010	011	100	101	110	111

Предположим, от законного пользователя А требуется зашифровать текст «POSSIBLE» с помощью одноразового блокнота и отправить его своему партнеру Б. Представление двоичного значения этого открытого текста выглядит следующим образом:

P	O	S	S	I	B	L	E
101	100	110	110	010	000	011	001

При шифровании в методе одноразового блокнота используется случайно выбранный ключ, равный длине открытого текста. Зашифрованный текст генерируется с применением операции XOR открытому тексту и ключу (*P – открытый текст, K – ключ* и *C – зашифрованный текст*): $C = P \oplus K$. Операция XOR ($\oplus$) приведена ниже:

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Из таблицы видно, что уравнение $x \oplus y \oplus y = x$ уместно. Это указывает на то, что при расшифровке с одноразовым паролем для зашифрованного текста достаточно генерация ключа операцией XOR: $P = C \oplus K$.

Предположим, что сторона А имеет следующий ключ, равный длине открытого текста в табл. 3.2:

111 101 110 101 111 100 000 101

Сторона А вычисляет зашифрованный текст на основе этого ключа следующим образом:

	P	O	S	S	I	B	L	E
Открытый текст	101	100	110	110	010	000	011	001
Ключ	111	101	110	101	111	100	000	101
Зашифрованный текст	010	001	000	011	101	100	011	100
	I	E	B	L	P	O	L	O

Шифр, отправленный А, легко расшифровывается с использованием того же ключа на стороне Б:

	I	E	B	L	P	O	L	O
Зашифрованный текст	010	001	000	011	101	100	011	100
Ключ	111	101	110	101	111	100	000	101
Открытый текст	101	100	110	110	010	000	011	001
	P	O	S	S	I	B	L	E

3.2. Симметричные криптографические алгоритмы

Ниже мы остановимся на симметричных криптосистемах, а также на двух их типах: *потоковом* и *блочном* симметричных алгоритмах шифрования. В алгоритмах симметричного шифрования используется один ключ для шифрования и расшифровки данных. Порядок осуществления процессов шифрования и расшифровки данных выбирается в зависимости от характера используемой системы.

При знакомстве с функционированием симметричных криптосистем вводятся следующие определения:

- шифрование открытого текста P симметричным ключом K: $C = E(P, K)$;

- расшифровка зашифрованного текста C симметричным ключом K: $M = D(C, K)$.

Здесь, $E()$ и $D()$, соответственно, являются функциями шифрования и расшифровки в симметричной криптосистеме.

Поточные симметричные алгоритмы шифрования. Потоковые симметричные алгоритмы шифрования основаны на одноразовом блокноте, разница заключается в том, что они имеют достаточно низкий уровень устойчивости и наличие управляемого ключа. То есть из ключа небольшой длины формируется последовательность, равная длине открытого текста, и используется в качестве одноразового блокнота.

Поточный шифр принимает ключ K с n битом и расширяет его до последовательности S, равной длине открытого текста. Зашифрованный текст C последовательности S вместе с открытым текстом P генерируется с помощью операции XOR. При этом, добавление последовательности выполняется так же, как добавление одноразового блокнота.

Поточный шифр можно записать в простом виде следующим образом:

$$StreamCipher(K) = S,$$

где K- ключ; S- полученная последовательность. Следует помнить, что в данном случае последовательность не зашифрованный текст, а простая строка, похожая на одноразовый блокнот.

Ели заданы последовательность $S = s_0, s_1, s_2, \ldots$, и открытый текст $P = p_0, p_1, p_2, \ldots$, то соответствующие биты $C = c_0, c_1, c_2, \ldots$, шифртектса с помощью операции XOR можно генерировать следующим образом.

$$c_0 = p_0 \oplus s_0, c_1 = p_1 \oplus s_1, c_2 = p_2 \oplus s_2 , \ldots$$

Для расшифровки зашифрованного текста C снова используется последовательность S:

$$p_0 = c_0 \oplus s_0, p_1 = c_1 \oplus s_1, p_2 = c_2 \oplus s_2 , \ldots$$

Обеспечивая отправителя и получателя одним и тем же алгоритмом шифрования потока, и ключом K, одинаковые последовательности могут быть сгенерированы с обеих сторон. Однако полученный шифр не имеет гарантированной безопасности, и основное внимание уделяется практическому применению.

Алгоритм поточного шифрования A5/1. Этот алгоритм поточного шифрования используется для обеспечения конфиденциальности данных в мобильных системах связи GSM. Хотя этот алгоритм имеет алгебраическую структуру, его можно даже представить в виде простой диаграммы.

Алгоритм шифрования A5/1 состоит из трех *регистров линейного сдвига*, которые обозначаются как *X, Y и Z,* соответственно. Регистр X содержит 19 битов $(x_0, x_1, \dots, x_{18})$, регистр Y 22 бита $(y_0, y_1, \dots, y_{21})$ и регистр Z 23 бита $(z_0, z_1, \dots, z_{22})$ информации. Неслучайно в трех регистрах хранятся биты такого размера. Это потому, что регистры линейного сдвига хранят в общей сложности 64 бита. Ключ *K*, используемый в алгоритме шифрования A5/1, имеет длину 64 бита, и этот ключ используется для первоначального заполнения регистров. Затем на основе алгоритма поточного шифрования генерируются последовательности требуемой длины (равной длине открытого текста). Прежде чем приступить к изучению порядка обобщения последовательностей, некоторые сведения о регистрах можно найти ниже.

В регистре сдвига X выполняется следующая последовательность операций:

$$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18},$$
$$x_i = x_{i-1} \text{ для } i = 18,17,16, \dots,1,$$
$$x_0 = t.$$

Аналогично, для регистров Y и Z также можно записать следующее:

$$t = y_{20} \oplus y_{21},$$
$$y_i = y_{i-1} \text{ учун } i = 21,20,19, \dots,1 \; y_0 = t$$

и

$$t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22},$$
$$z_i = z_{i-1} \text{ учун } i = 22,21,20, \dots,1,$$
$$z_0 = t.$$

Для заданных трех битов x, y и z значение функции $maj(x, y, z)$ равно максимальному количеству битов. Например, если x, y и z биты равны 0, то значение функции равно 0. Поскольку входящие в функцию биты нечетные, функция всегда возвращает 0 или 1. Других случаев не будет.

В шифре A5/1 для генерации каждого бита последовательности выполняется следующее. Сперва вычисляется значение функции $m = maj(x_8, y_{10}, z_{10})$. После X, Y и Z регистры сдвигаются следующим образом (или не сдвинутся):

– если $x_8 = m$, сдвигается X;

– если $y_{10} = m$, сдвигается Y;

– если $z_{10} = m$, сдвигается Z.

Один бит s последовательности генерируется следующим образом:

$$s = x_{18} \oplus y_{21} \oplus z_{22}.$$

Приведенные выше операции последовательности, повторяются по мере необходимости (равной длине открытого текста или зашифрованного текста).

Если регистр сдвигается, его полное состояние изменится. При формировании одного бита последовательности, по крайней мере, два из трех регистров сдвигаются, и поэтому можно создать новую последовательность битов, продолжая указанную выше последовательность.

Хотя алгоритм поточного шифрования A5/1 выглядит сложным, высокая скорость проявится при реализации на устройстве. В общем случае поточный шифр A5/1 можно представить, как показано на рис. 3.4.

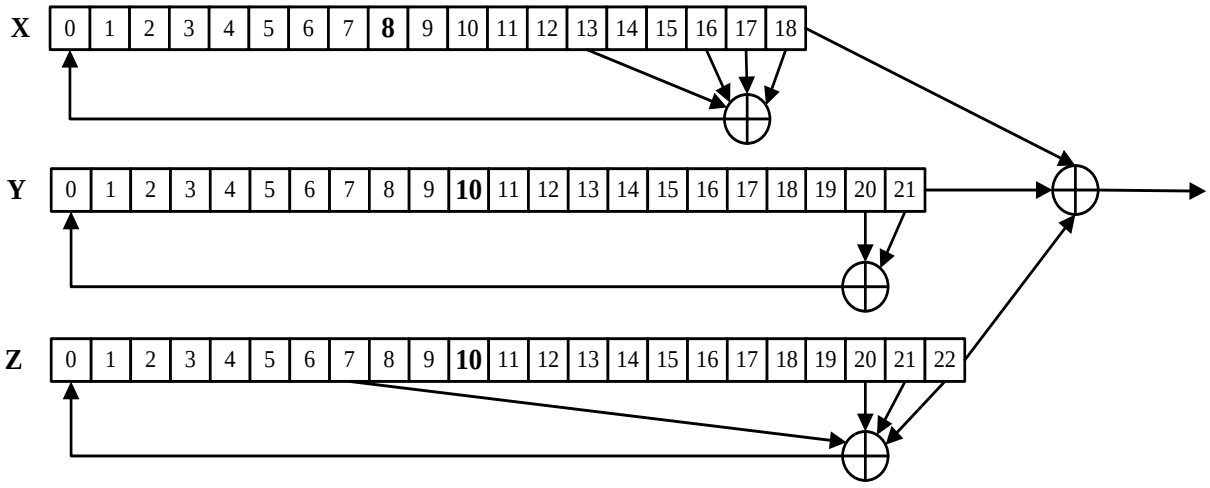


Рис.3.4. **Общий вид генератора последовательности A5/1**

Пример. Предположим, что результат записи 64-битного ключа K в регистры X, Y и Z имеет следующий вид (рис. 3.5).

В этом случае $maj(x_8, y_{10}, z_{10}) = maj(1,1,0) = 1$ и это указывает на сдвиг регистров X и Y. Следовательно,

$$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18} = 0 \oplus 1 \oplus 1 \oplus 1 = 1,$$
$$x_i = x_{i-1} \text{ для } i = 18,17,16, \ldots,1,$$
$$x_0 = 1.$$

Аналогично, также для регистра Y можно записать следующее:

$$t = y_{20} \oplus y_{21} = 0 \oplus 0 = 0,$$
$$y_i = y_{i-1} \text{ для } i = 21,20,19, \ldots,1,$$
$$y_0 = 0.$$

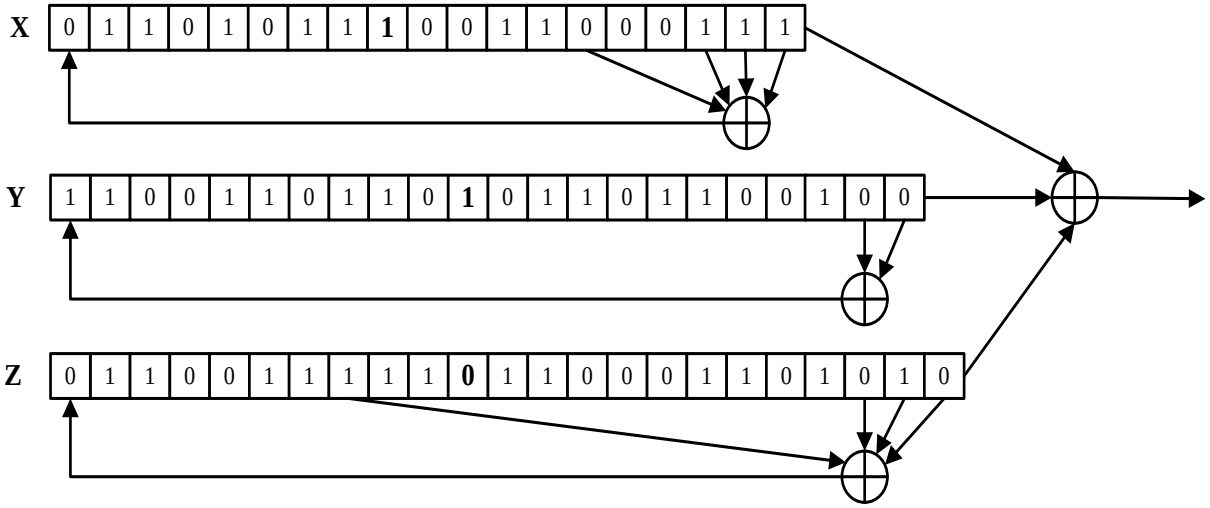


Рис.3.5. **Начальное состояние регистров *X*, *Y* и *Z***

Состояние после сдвига регистров X и Y имеет следующий вид (рис. 3.6):

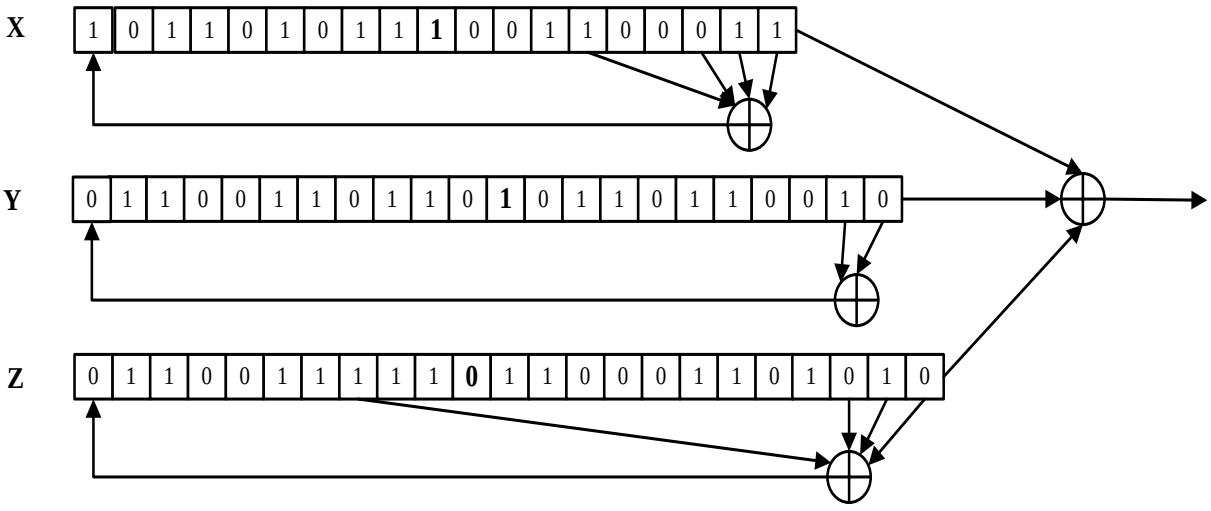


Рис.3.6. **Состояние, после сдвига регистров *X*, *Y* и *Z***

$s = x_{18} \oplus y_{21} \oplus z_{22} = 1 \oplus 0 \oplus 0 = 1$ один бит, генерируемый из состояния последнего регистра после сдвига. В этом порядке генерируется необходимая последовательность битов.

Алгоритмы потокового шифрования были очень популярны в то время, когда вычислительные устройства не были такими продвинутыми, как сегодня, и сегодня их заменяют симметричные блочные шифры. Однако, бывают такие случаи, когда потоковые шифры, несомненно, будут необходимы. Например, одна из систем реального времени в сети GSM не имеет возможности использовать блочные симметричные шифры при шифровании данных. Это связано с тем, что блок (длина блока будет не менее 64 бит), необходимый для шифрования, должен быть собран в определенное время. Это приводит к паузам в разговоре. Кроме того, считается, что симметричное поточное шифрование устойчиво к изменениям в зашифрованном тексте (в результате внешних воздействий) в процессе передачи зашифрованных данных. Например, при поточном шифровании изменение одного бита в зашифрованном тексте также приводит к изменению одного бита в открытом тексте. В симметричных блочных шифрах изменение одного бита приводит к изменению одного блока (например, 64 бита). Кроме того, симметричное поточное шифрование может выполняться на устройствах меньшего размера, чем блочное шифрование.

Блочные алгоритмы симметричного шифрования. Повторяющееся блочное шифрование разбивает открытый текст на блоки ограниченной длины. В большинстве блочно-симметричных шифров зашифрованный текст получается путем повторения функции открытого текста F в течение нескольких *раундов*. Функция F на основе результата и ключа K из предыдущего раунда называется *функцией раунда 1*. Основная причина такого наименования заключается в том, что оно выполняется в течение многих раундов.

Основной целью создания блочных симметричных шифров является достижение безопасности и эффективности. Создание безопасных или эффективных блочных шифров не является сложной задачей. Однако, создание безопасных и эффективных симметричных блочных шифров – *это искусство*.

Для создания симметричных блочных шифров используется много сетей. На практике широко используются следующие сети:

1. Сеть Фейстеля.
2. Сеть SP (Substitution – Permutation network).
3. Сеть Лаи-Массей.

Сеть Фейстеля – является общим принципом симметричного блочного шифрования, а не только одного блочного шифра. Согласно сети Фейстеля, блок открытого текста P разделяется на две разные левую и правую части:

$$P = (L_0, R_0),$$

и для каждого раунда $i = 1,2, \dots, n$, новые левые и правые стороны рассчитываются в соответствии со следующим правилом:

$$L_i = R_{i-1},$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i).$$

Здесь ключ K_i – *частичный ключ* (ключ раунда) для i - раунда. Частичные ключи, в свою очередь, вычисляются с помощью алгоритма генерации ключа из ключа K. Итоговый блок зашифрованного текста C равен результату последнего раунда, т.е.:

$$C = (L_n, R_n).$$

Расшифровка в сети Фейстеля основана на «волшебстве» операции XOR. То есть для $i = n, n-1, \dots, 1$ выполняется следующее уравнение:

$$R_{i-1} = L_i,$$
$$L_{i-1} = R_i \oplus F(R_{i-1}, K_i).$$

Результат последнего раунда дает расшифрованный текст: $P = (L_0, R_0)$.

В сети Фейстеля функция F, используемая в каждом раунде, не обязательно должна иметь обратимой. Однако любая полученная F функция не может быть полностью безопасной. К симметричным блочным шифрам можно привести такие примеры как AES, DES, ГОСТ Р 28147-89, O'z Dst 1105:2009, IDEA, Blowfish и др.

Проблемы в симметричных криптосистемах. Системы симметричного шифрования используют один и тот же ключ для шифрования и расшифровки данных. Это, в свою очередь, требует передачи ключа шифрования перед передачей зашифрованных данных по сети. Другими словами, *безопасная передача ключей*

между сторонами является основной проблемой, стоящей перед симметричными криптосистемами.

Кроме того, при передаче данных от одного пользователя к другим, требуется наличие отдельных ключей для работы с каждым из них. Это приводит к необходимости безопасного хранения большого количества ключей пользователя.

Длина ключа в симметричных криптосистемах. На практике к длине ключа криптографических систем предъявляются строгие требования. Эти требования меняются со временем, в зависимости от изменения возможностей вычислительных устройств. Необходимо, чтобы не было возможности узнать ключ, используемый в криптосистемах, вычисляя его через вычислительные устройства текущего времени. Здесь, когда говорится о нахождении ключа, подразумевается вычислить все возможные варианты ключа заданной длины. Например, если длина ключа равна 4 битам, то число возможных вариантов будет равно $2^4 = 16$, или, в общем случае, варианты, которые могут быть n битными ключами, будут равны 2^n.

В настоящее время длина ключей, используемых в симметричных криптосистемах, должна составлять не менее 128 бит. В табл. 3.3 показано время, затраченное на использование устройств, с различными значениями для расчета всех возможных вариантов ключей разной длины. Отображенные результаты приведены на основе цен 2005 года.

Таблица 3.3

Время расчета всех вариантов ключей разной длины

Длина ключа / **Стоимость устройства**	**80 бит**	**112 бит**	**128 бит**
10 000 $	7 000 лет	10^{13} лет	10^{18} лет
100 000 $	700 лет	10^{12} лет	10^{17} лет
1 000 000 $	70 лет	10^{11} лет	10^{16} лет
10 000 000 $	7 лет	10^{10} лет	10^{15} лет
100 000 000 $	245 дней	10^{9} лет	10^{14} лет

3.3. Криптосистемы с открытым ключом

Одна из существующих проблем в симметричных криптосистемах – безопасная передача и хранение секретного ключа. Ниже приведены так называемые асимметричные или криптосистемы с открытым ключом, в которых устраняются проблемы, связанные с передачей и безопасным хранением ключей.

В криптосистемах с открытым ключом, шифрование данных осуществляется с помощью одного ключа (называемого открытым ключом), а его расшифровка осуществляется с помощью другого ключа (называемого закрытым ключом). Поэтому, в криптосистемах с открытым ключом устраняется проблема распределения ключей, присутствующих в симметричных криптосистемах. Однако криптографические системы с открытым ключом также имеют свойственные им проблемы.

При создании криптосистем с открытым ключом основываются на *односторонних функциях с «ловушками»*. Здесь смысл словосочетания «односторонний» означает, что функция легко вычисляется односторонне. Однако вычисление противоположности этой функции гораздо сложнее (то есть вычислить ее невозможно). Основная причина, по которой его здесь называют «ловушкой», заключается в том, что злоумышленник не может использовать открытую информацию (например, открытый ключ) при восстановлении личной информации (например, закрытого ключа). В качестве примера этих односторонних функций можно показать операцию факторизации. То есть легко сгенерировать два простых числа p и q и вычислить $N = p * q$. Однако, когда число N достаточно велико, сложно выразить его как произведение двух простых чисел, и это требует высокой вычислительной мощности.

В шифрах с симметричным ключом было условлено, что если открытый текст P зашифрован, генерируется шифр C. В системах шифрования с симметричным ключом было введено условие, что если сообщение M зашифровано, генерируется шифр C.

Чтобы использовать криптографические системы с открытым ключом, сторона Б должна иметь *открытый ключ* и соответствующую ему пару *закрытых ключей*. Зашифровать информацию может тот, кому известен открытый ключ стороны Б. Вскрытие зашифрованного сообщения допустимо только стороне Б, являющегося владельцем закрытого ключа.

Модульная арифметика. Поскольку криптосистемы с открытым ключом основаны в основном на модульной арифметике, она будет рассмотрена в первую очередь.

Деление всякого целого числа на $m_{\in} z$, соответствует остатку, присвоенному этому числу. Например, $\frac{5}{2} = 2 * 2 + 1$, где остаток равен 1, а целая часть равна 2. В криптографии, если остаток числа a при делении на число b равен числу r, он обозначается следующим образом: $amodb \equiv r$. А в языках программирования обозначается как $a\%b$.

Ниже приведены несколько примеров остаточной арифметики:

– $7mod3 \equiv (3 * 2)mod3 + 1mod3 \equiv 0 + 1 \equiv 1;$

– $14mod3 \equiv (3 * 4)mod3 + 2mod3 \equiv 0 + 2 \equiv 2;$

– $2mod3 \equiv (0 * 3)mod3 + 2mod3 \equiv 2;$

– $5mod7 \equiv 5;$

– $-2mod5 \equiv (-2 + 5)mod5 \equiv 3mod5 \equiv 3;$

– $-7mod3 \equiv (-7 + 3)mod3 \equiv -4mod3 \equiv (-4 + 3)mod3 \equiv -1mod3 \equiv (-1 + 3)mod3 \equiv 2.$

Кроме того, в криптографии с открытым ключом важно вычислить обратное число по модулю. Например, в традиционной математике число, обратное к числу a, равно $\frac{1}{a}$, в то время как в модульной арифметике число, обратное числу a в n модулях, обозначается как $a^{-1}modn.$

Также как и в традиционной математике, произведение числа на обратное равно единице, и в модульной арифметике произведение числа на обратное также равно единице. То есть, если $a^{-1}modn \equiv b$, тогда уместно равенство $(a * b)modn \equiv 1.$

Примечание. В криптографии в качестве модуля (то есть делителя) требуется использовать только простые числа. То есть n в уравнении amodn всегда должно быть простым.

Предположим, требуется найти обратное число 3 в модуле 7. То есть требуется найти x: $3^{-1}mod7 \equiv x$. Используя приведенное выше уравнение $(3 * x)mod7 \equiv 1$, результат можно вычислить, подставив число вместо x. Но этот процесс требует много времени (особенно с большими числами).

Алгоритм RSA. Название RSA происходит от первых букв фамилий создателей алгоритма (Rivest, Shamir и Adleman).

Алгоритм RSA основан на использовании операции арифметического возведения в степень.

В алгоритме RSA для генерации пары открытых и закрытых ключей выбираются два числа большой длины p и q, и вычисляется их умножение: $N = p * q$. После этого выбирается число e, которое является взаимно простое с $\varphi(N) = (p-1) * (q-1)$ (значение функции $\varphi(N)$ приведено ниже). Затем в модуле $\varphi(N)$ вычисляется обратное число e, и оно приравнивается на d. Также, существуют числа e и d, удовлетворяющие умножение N двух простых (p и q) чисел и условие $ed = 1\, mod\, \varphi(N)$. После этого p и q забываются (удаляются).

Здесь N - модуль, составляющий (N, e) - пары открытых ключей, и d - секретного ключа. Для шифрования в алгоритме RSA сообщение M должно быть выражено в числовой форме, а N возводиться по модулю до степени e, то есть

$$C = M^e\, mod\, N.$$

Для расшифровки C, требуется возводить закрытый ключ по модулю N до степени d:

$$M = C^d\, mod\, N.$$

Другими словами, если в алгоритме RSA сообщение зашифровано открытым ключом и расшифровано закрытым ключом, необходимо доказать правильность уравнения $M = C^d\, mod\, N = M^{ed}\, mod\, N$.

Допустим, что в алгоритме RSA требуется выполнить операции шифрования и расшифровки данных над выбранными «большими» ($p = 11$ и $q = 3$) числами. В этом случае модуль будет равен $N = p * q = 33$ и $\varphi(N) = (p-1)(q-1) = 20$. В этом случае степень e, требуемая для шифрования, может быть принята равной 3. Причина в том, что число 3 взаимно простое с $\varphi(N) = 20$. После этого, на основе расширенного алгоритма Евклида, определяется ключ расшифровки $d = 7$. То есть, $ed = 3 * 7 = 1\, mod\, 20$. В этом случае пара открытых ключей стороны А будет равна $N, e = 33, 3$, а закрытый ключ d будет равен 7.

После этого сторона А передает всем свой открытый ключ. Однако хранит закрытый ключ в секрете.

Предположим, что сторона Б хочет отправить информацию $M = 15$ стороне А в зашифрованном виде. Для этого сторона Б

берет пару открытых ключей $N, e = 33,3$ стороны А и вычисляет зашифрованный текст следующим образом:

$$C = M^e \; mod \; N = \; 15^3 = 3375 = 9 \; mod \; 33$$

и отправляет его стороне А.

Сторона А для расшифровки зашифрованного текста использует закрытый ключ $d = 7$:

$M = C^d \; mod \; N = 9^7 = 4782969 = 144938 * 33 + 15 = 15 \; mod \; 33.$

Если в алгоритме RSA используются небольшие простые числа (для p и q), злоумышленник может легко записать открытое N в виде произведения двух простых чисел. Затем, используя вторую часть открытого ключа e, может вычислить закрытый ключ d. Поэтому для практического использования алгоритма RSA требуется, чтобы длина выбранных простых чисел была не менее 2048 бит. Кроме того, не было доказано, что взлом алгоритма RSA связан только с проблемой факторизации.

Использование криптосистем с открытым ключом. При рассмотрении вопроса об использовании криптографических систем с открытым ключом вводятся следующие определения:

Шифрование сообщения M с открытым ключом стороны А: $C = \{M\}_A$.

Расшифровка зашифрованного текста с закрытым ключом стороны A: $M = [C]_A$.

Исходя из этого можно спокойно написать следующее уравнение: $[\{M\}_A]_A = M$. Другими словами, если сообщение M зашифровать с открытым ключом стороны А, а затем расшифровывать его закрытым ключом этой же стороны, сгенерируется исходное сообщение.

Произвольную операцию, выполненную с симметричными шифрами, также можно выполнять с помощью алгоритмов шифрования с открытым ключом. Например, в небезопасной среде при передаче информации в сети, для обеспечения конфиденциальности информации вместе симметричных алгоритмов шифрования могут использоваться криптографические алгоритмы с открытым ключом. Однако процесс требует большего времени.

Кроме того, криптосистемы с открытым ключом, такие как симметричные криптосистемы, также могут использоваться для обеспечения целостности данных.

Криптосистемы с открытым ключом преодолели проблему распределения ключей, существующих в симметричных криптосистемах. В свою очередь, симметричные криптосистемы отличаются своей эффективностью по сравнению с криптосистемами с открытым ключом. Другими словами, в симметричных криптосистемах операции шифрования и расшифровки выполняются быстрее, чем в алгоритмах шифрования с открытым ключом.

Существует ли возможность совместить преимущества обеих криптосистем? То есть, возможно ли создать криптосистему, которая будет высокоэффективна при шифровании данных, и не иметь проблем с распределением ключей? Конечно, это возможно, и такие системы называют *гибридными* криптосистемами. В гибридных криптосистемах ключ к алгоритму симметричного шифрования доставляется через шифрование с открытым ключом, а сами данные защищены симметричным шифрованием. Схема гибридной криптосистемы отображена на рис. 3.7.

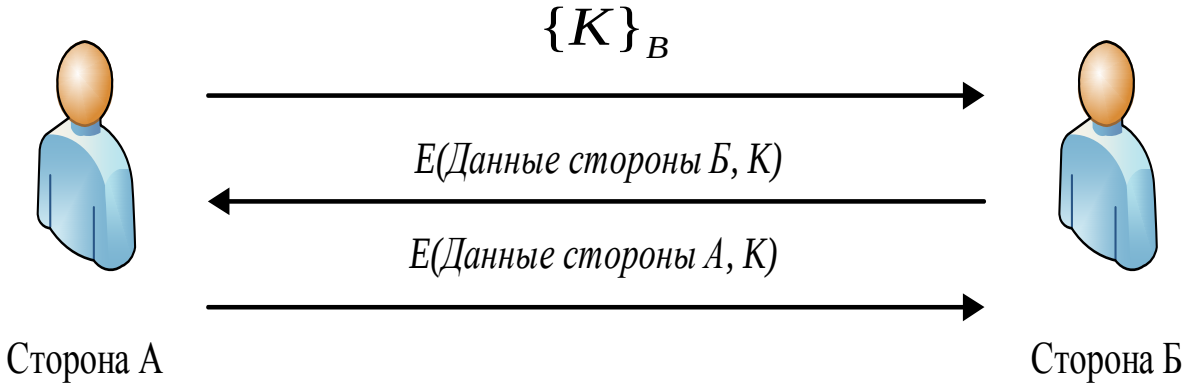


Рис.3.7. **Гибридная криптосистема**

Длина ключа в криптосистемах с открытым ключом. Как и в криптосистемах с симметричным ключом, криптосистемы с открытым ключом требуют длины ключа для использования в реальной жизни. Этот вопрос обсуждался выше для симметричных криптосистем. Поскольку математическая основа симметричных и открытых криптосистем различна, они будут иметь различную длину ключа, когда находятся на одном и том же уровне устойчивости (табл.3.4).

Таблица 3.4

Длина ключей симметричных и открытых криптосистем с одинаковой устойчивостью

Алгоритм симметричного шифрования	Алгоритм RSA (числа p и q)
56 бит	512 бит
80 бит	1024 бит
112 бит	2048 бит
128 бит	3072 бит
192 бит	7680 бит
256 бит	15360 бит

Как и в симметричных криптосистемах, в криптосистемах с открытым ключом все варианты ключей зависят от способности устройств выполнять вычисления. То есть длина ключа, которая в настоящее время считается достаточной, может быть не рекомендована через 10 лет. Поскольку в течение 10 лет возможности вычислительных устройств не будут такими же, как сейчас.

В табл. 3.5 показаны значения времени, необходимые для факторизации в различной длине модулей N в алгоритме RSA. В этом случае результаты были получены за счет компьютера, выполняющего миллион операций в секунду (*one-million-instruction-per-second, mips*) или 10^{13} операций в год. В качестве алгоритма факторизации использовался GNFS (general number field sieve).

Из приведённых выше данных видно, что увеличение возможностей вычислительных устройств, приводит к снижению устойчивости криптографических алгоритмов. Это относится как к симметричным криптосистемам, так и к криптосистемам с открытым ключом.

Таблица 3.5

Значения времени, необходимые для факторизации на разных длинах модуля N в алгоритме RSA

Длина N в битах	Требуемые годы
512	30 000
768	$2*10^8$
1024	$3*10^{11}$
1280	10^{14}
1536	$3*10^{16}$
2048	$3*10^{20}$

3.4. Методы обеспечения целостности данных

Оба алгоритма шифрования (симметричный и с открытым ключом) были упомянуты только для использования обеспечения конфиденциальности данных. Ниже можно ознакомиться с вопросом их использования при проверке целостности информации.

Хэш-функция – функция, отображающая входное слово конечной длины в конечном алфавите в слово заданной, обычно фиксированной длины. Хэш-функция имеет следующие свойства:

1. Можно применять к тексту произвольной длины.
2. На выходе формируется значение заданной длины.
3. Для произвольного x, $h(x)$ легко вычисляется.
4. Для произвольного H, с уравнения $h\,(x) = \mathrm{H}$ невозможно вычислить x (свойство односторонности).
5. Для полученных x и $y \neq x$ текстов получится $h(x) \neq h(y)$ (свойство устойчивости к коллизии).

Простой вид проверки целостности передаваемых данных с помощью хэш-функции приведен на рис. 3.8. Отправитель вычисляет хэш-значение сообщения и отправляет его получателю вместе с сообщением. Получатель сначала вычисляет хеш-значение сообщения и сравнивает его с полученным хэш-значением. Если оба хэш-значения равны, целостность данных не изменена, в противном случае она считается измененной. Обычно хэш-функцию еще называют *бесключевой криптографической функцией*, так как хэш при вводе кроме данных не требует никакого значения (существуют также методы обеспечения целостности информации, требующие ключа).

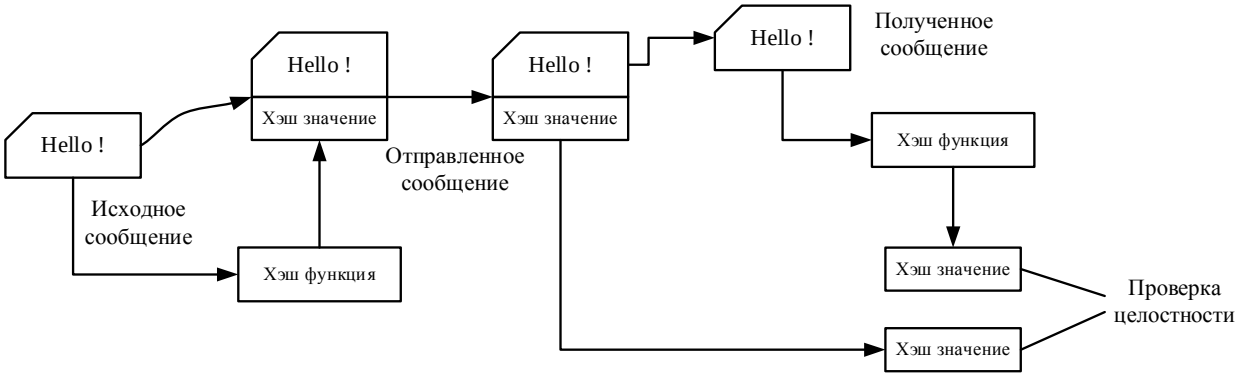


Рис.3.8. **Проверка целостности данных на основе хэш-функции**

Поскольку проблема безопасности в вышеупомянутом методе серьезна, на практике она не используется. То есть у злоумышленника есть возможность проверить целостность только при изменении информации. Однако, злоумышленник может легко убедить пользователя в целостности данных, обменяв хэш-значение данных.

Существует *MAC* (*message authentication code)* система, устраняющая эту проблему, согласно которой хэш-значение данных вычисляется на основе секретного ключа (рис. 3.9).

При разработке системы MAC также можно использовать блочные шифры. Для этого достаточно использовать блочный шифр в режиме CBC (Cipher Block Chaining – цепочка шифроблоков) и получить последний зашифрованный блок (остальные будут выброшены).

Конечно, этот метод – не единственный способ создания системы MAC. Ниже можно познакомиться с созданием системы MAC на основе хэш-функций.

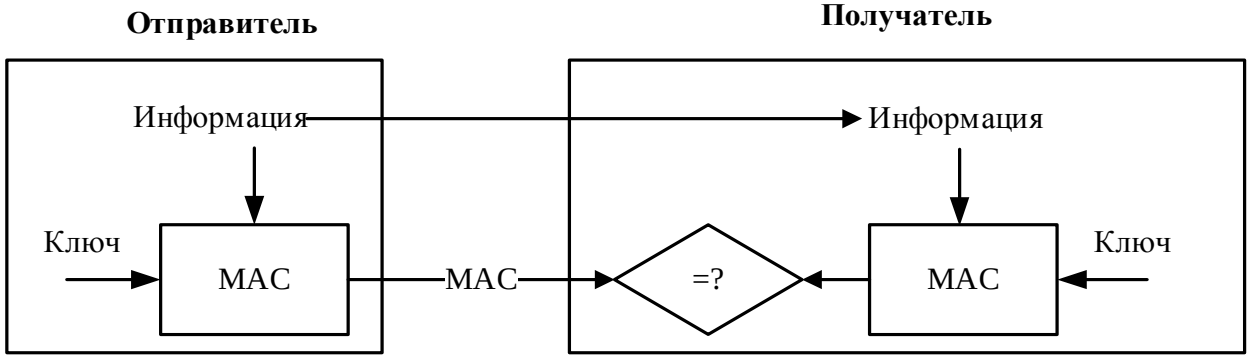


Рис.3.9. **Система MAC**

Проверка целостности данных на основе хэш-функций. Выше было заявлено о недостатке реализации вычисления $h(M)$ при проверке целостности данных M и отправке $M, h(M)$ получателю. Поэтому на практике хэш-функции напрямую не используются для обеспечения целостности данных. Другими словами, цель состоит в том, чтобы гарантировать, что вычисленное хэш-значение не может быть изменено при обеспечении целостности данных на основе хэш-функций. Для ее реализации, возможно, необходимо зашифровать хэш-значение на основе симметричного ключа шифрования (то есть $E(h(M), K)$). Однако, существует более простой способ сделать это – методом

хешированного MAC (hashed MAC или HMAC). Согласно этому методу, вместо шифрования хэш-значения, ключ непосредственно прикрепляется к данным в процессе вычисления хэш-значения. Как прикрепляются ключи в системе HMAC? В общем случае с двумя методами: вставка ключа перед текстом ($h(K, M)$) или вставка ключа после текста ($h(M, K)$), в каждой из них имеются серьезные проблемы с безопасностью.

Хэш-функции также являются криптосистемами и при хэшировании информации, как и в симметричном блочном шифровании, разбиваются на блоки. Обычно для большинства хэш-функций (например, MD5, SHA1, Tiger) длина блока равна 64 байтам или 512 битам.

В системе *HMAC* ключ прикрепляется к данным следующим образом. Сперва длина блока в хэш-функции определяется в байтах. Допустим, в хэш-функции MD5 длина блока равна $B = 64$ байтам. Длина полученного ключа (K) также приравнивается к длине блока. Здесь может быть 3 случая: (1) если длина ключа равна 64 байтам, то никакое изменение не произойдет, (2) если длина ключа меньше 64, то отсутствующие байты заменяются нулями, (3) если длина ключа больше длины блока, то ключ сперва хэшируется, и правая часть сгенерированного значения хэш-функции заполняется нулями, пока не достигнет длины блока. Таким образом, длина ключа приравнивается к длине блока.

Следовательно, на основе данных и приспособленного ключа, значение HMAC вычисляется следующим образом:

$$HMAC(M, K) = H\big(K \oplus opad, H(K \oplus ipad, M)\big),$$

где $ipad$ и $opad$ переменные генерируются следующим образом:

$$ipad = \text{в результате повторения } 0x36 \ \ B \text{ раз},$$

$$opad = \text{в результате повторения } 0x5c \ \ B \text{ раз}.$$

Как видно из уравнения, в HMAC выполняется двойное хэширование. Поскольку ключ K известен только двум сторонам (отправителю и получателю), злоумышленник не может пересчитать соответствующее хэш-значение. Из пар данных, отправленных со стороны A ($M, HMAC(M, K)$), злоумышленник может только изменить данные, и эта ситуация легко обнаруживается получателем.

Проверка целостности данных и защита от отказа на основе алгоритмов шифрования с открытым ключом. Ниже

можно познакомиться с системой *электронной цифровой подписи*, основанной на криптосистемах с открытым ключом и хэш-функциях. В Законе Республики Узбекистан «Об электронной цифровой подписи» к электронной цифровой подписи дано следующее определение:

«*Электронная цифровая подпись (ЭЦП)* – подпись в электронном документе, полученная в результате специальных преобразований информации данного электронного документа с использованием закрытого ключа электронной цифровой подписи и позволяющая при помощи открытого ключа электронной цифровой подписи установить отсутствие искажения информации в электронном документе и идентифицировать владельца закрытого ключа электронной цифровой подписи».

Электронная цифровая подпись, как и простая собственноручная подпись, ставится только в электронных документах и обеспечивает целостность подписанной информации и гарантирует, что подписавший не откажется от подписанной подписи. В информационной безопасности существует *проблема отказа*, согласно которой пользователь отказывается от собственноручно подписанного документа (т.е. настаивает на том, что он не подписывал). Именно для предотвращения этой проблемы используются системы электронной цифровой подписи.

Таким образом, системы ЭЦП не только обеспечивают целостность информации, но и препятствуют (или предотвращают отказ) уклонению подписывающего лица от выполнения обязательств. Таким образом, системы ЭЦП отличаются от систем MAC, основанных на симметричных криптосистемах, обеспечивающих целостность данных.

В системах MAC чтобы не иметь возможность пересчитывать хэш-значение к тексту прикреплен ключ, в системах ЭЦП «шифрование» осуществляется с закрытым ключом хэш-значения информации и генерируется ЭЦП. Чтобы «расшифровать» это сообщение, достаточно знать открытый ключ стороны. Следовательно, она похожа на простую систему подписи (в простой системе подписи подписывает один человек, и от остальных требуется проверка ее подлинности). В системе ЭЦП владелец закрытого ключа также подписывает сообщение, а остальные проверяют подлинность подписи, используя его открытый ключ.

Если сторона А подписывает сообщение M, то подпись выражается в виде $S = [M]_A$ (также, как и расшифровка с закрытым ключом в криптографии с открытым ключом). Создание систем ЭЦП состоит из двух процедур: *Формирование ЭЦП* и *Проверка ЭЦП* (рис. 3.10).

Процесс формирования ЭЦП. Допустим, требуется от стороны А подписать сообщение M. Для этого вычисляется хэш-значение сообщения M: $H = h(M)$. Затем хеш-значение сообщения H «шифруется» с помощью закрытого ключа пользователя (это не настоящее шифрование, оно просто заключается в выполнении операции над H с закрытым ключом) и генерируется подпись $S = [H]_A$. Сгенерированная подпись прикрепляется к данным $\{M, S\}$ и передается получателю.

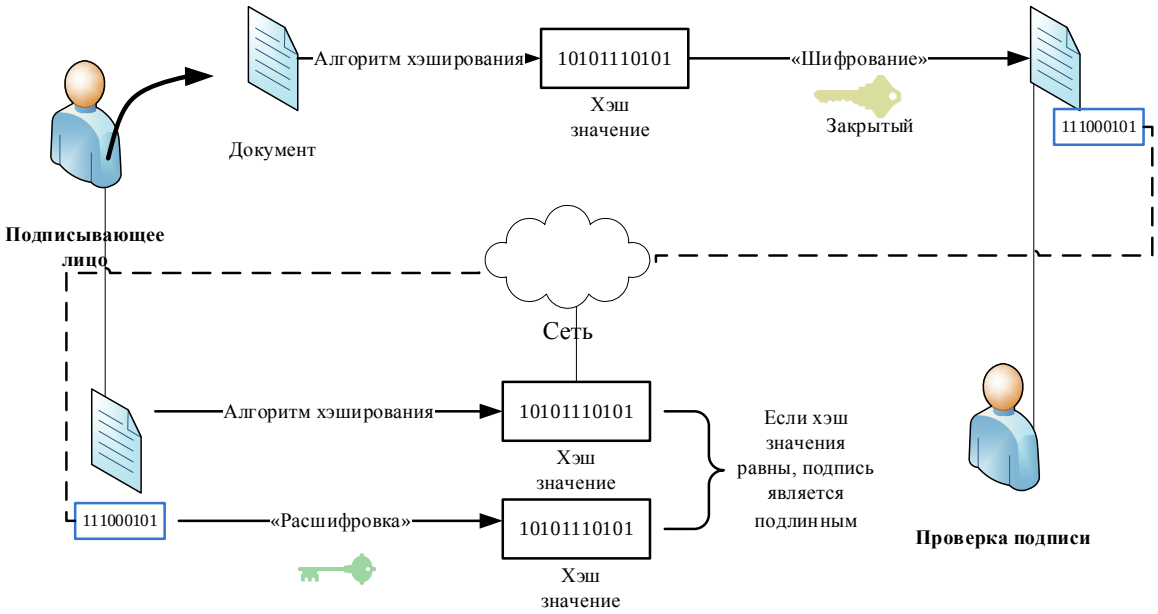


Рис.3.10. **Схема электронной цифровой подписи**

Процесс проверки ЭЦП. Допустим, требуется от стороны B проверить подпись S, подписанное в сообщении M'. Для этого B сторона сперва вычисляет хэш-значение сообщения M': $H' = h(M')$. С открытым ключом стороны A «расшифровывается» S (это не настоящая расшифровка, она просто заключается в выполнении операции над S с открытым ключом) и генерируется H. Если оба хэш-значения (H и H') взаимно равны, ЭЦП считается правильным (следовательно, сообщение целое).

Прежде чем разобраться в защите от отказа, приведем простой пример обеспечения целостности на основе MAC. Допустим,

сторона A своему диллеру со стороны B подал заявку на 100 акций. Чтобы гарантировать целостность данного заказа, сторона A с помощью распределенного ключа K_{AB} стороны B вычисляет MAC. Через определенное время заказы будут готовы. Однако цена акций упадет до того, как сторона A произведет платеж. В это время сторона A будет настаивать на том, что она не заказывала и отвергает платеж. Это связано с тем, что обе стороны генерируют рассчитанный MAC, для обеспечения целостности.

Если такая ситуация осуществляется с ЭЦП? В этом случае, сторона A подписывает заказ своим закрытым ключом и отправляет его стороне B. Здесь сторона A не может отрицать о поданной заявке. Причина в том, что подписание заказа осуществляется только закрытым ключом. А секретный ключ известен только стороне A.

Инфраструктура открытых ключей (Public key infrastructure, PKI). Еще одна проблема криптографии с открытым ключом – это определение того, кому принадлежит открытый ключ. Предположим, сторона A хочет отправить секретное сообщение M стороне B. Для этого сторона A использует открытый ключ стороны B. Однако сторона C со злым умыслом представляет свой открытый ключ стороне A как открытый ключ стороны B. Поскольку сторона A не может проверить эту ситуацию, она доверяет ей и шифрует секретное сообщение открытым ключом стороны C.

Чтобы избежать этой проблемы, криптографические системы с открытым ключом используют *инфраструктуру открытого ключа*.

Инфраструктура открытого ключа, или PKI, включает в себя все, что требуется для безопасного использования криптосистем с открытым ключом в реальной жизни. Взаимодействие всех компонентов PKI - очень сложный процесс, некоторые из их составляющих и основные функции PKI описаны ниже.

Цифровой сертификат (сертификат открытого ключа или краткий сертификат) состоит из имени пользователя и его открытого ключа (на практике также будет содержаться информация о пользователе и сертификате) и подписывается *центром сертификации* (*certificate authority* или *CA*). Например, сертификат стороны A состоит из:

$M = (\text{название стороны } A, \text{открытый ключ стороны } A)$ и $S = [M]_{CA}$.

Чтобы проверить этот сертификат сторона B вычисляет $\{S\}_{CA}$ и проверяет равенство на M.

Сторона CA обычно рассматривается как *доверенная третья сторона (trusted third party* ёки *TTP)*. То есть сторона A обычно генерирует пару закрытых и открытых ключей для пользователя. После того, как закрытый ключ предоставлен стороне A, он удаляется из CA. Открытый ключ предоставляется в виде сертификата. Если сторона B хочет отправить какую либо зашифрованную информацию для стороны A, она воспользуется ее сертификатом. Для этого требуется проверка подписи на сертификате. Это, в свою очередь, требует чтобы сторона B знала открытый ключ CA (то есть сертификат, эквавалентный ему). Таким образом, открытый ключ (или сертификат) стороны CA доступен в уже используемой системе и располагает всей информацией о нем.

3.5. Шифрование дисков и файлов

Криптографическая защита информации, в частности, алгоритмы шифрования, широко применяются на практике. В качестве примера можно привести шифрование данных на запоминающих устройствах или шифрование информации, передаваемой по сети. Как правило, для шифрования данных используется определенный алгоритм. Этот алгоритм может быть в виде приложения, разработанного для операционной системы (ОС) (например, Windows ОТ, Linux ОТ, Android ОТ) или специального устройства (например, специальных процессоров, токена USB, смарт-карты и т.д.).

На практике криптографические алгоритмы используются в качестве средств следующего вида:

- средства аппратно-программного вида;
- средства аппаратного вида;
- средства программного вида.

Аппаратно-программное шифрование – процесс шифрования с использованием специально разработанного вычислительного устройства. Примером может служить устройство шифрования ruToken USB (рис. 3.11).

Рис.3.11. **Устройство шифрования ruToken USB**

Устройство шифрования ruToken USB – устройство производства Российской Федерации, которое в основном реализовано в криптографических алгоритмах Российской Федерации. Общие характеристики разработанного устройства Рутокен S следующие:

- используется для безопасного хранения ключей шифрования, ключей ЭЦП и различных сертификатов;
- чтобы использовать этот токен, требуется ввести ПИН код;
- применяется для шифрования данных на диске;
- в токене имеются уровни гостя, пользователя и администратора;
- можно использовать в средах Microsoft Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/ XP/2003, GNU/Linux, Apple macOS/OSX;
- EEPROM с памятью 32, 64 и 128 КБ;
- имеет интерфейс USB 1.1 и выше;
- имеет размер 58x16x8мм (микро-токен 17,8x15,4x5,8мм);
- имеет вес 6,3г (микро-токен 1,6г).

Аппаратное шифрование имеет следующие специфические особенности:

- использует специальный процессор, расположенный в накопителе (устройстве);
- в процессоре имеется специальный генератор ключей для генерации ключа шифрования, который разблокируется на основе пароля, введенного пользователем;
- эффективность достигается за счет отказа от использования основной системы (системы, к которой подключено устройство, например, компьютер) для шифрования;

- ключи и другие секретные величины на устройстве защищены с помощью шифрования;

- аутентификация осуществляется относительно аппаратного устройства;

- обеспечивает высокую экономическую эффективность в разрезе средних и крупных организаций и простоту поддержки;

- постоянно доступная функция шифрования, реализованная на устройстве;

- нет необходимости устанавливать дополнительные драйверы или программное обеспечение;

- данные защищены от широко распространенных методов атаки, полного выбора пароля, атак на основе ввода вредоносных программ и атак, направленных на поиск ключа;

- реализация требует более высокой цены, чем программное средство.

Программное шифрование осуществляет процесс шифрования и расшифровки информации на дисках, файлах, каталогах и различных носителях посредством компьютера. В целом программные средства шифрования можно разделить на следующие группы:

- программные средства шифрования диска (Disk encryption software);

- программные средства шифрования файла/ каталога (File/folder encryption);

- программные средства шифрования базы данных (Database encryption);

- программные средства шифрования связи (Communication encryption software).

На рис. 3.12 показан вид программного средства TrueCrypt, используемого для шифрования диска. Это программное средство имеет следующие особенности:

- написано с использованием языков программирования C, C++, Assembly;

- можно использовать в ОС Windows, macOS и Linux;

- размер равен 3.30 MB;

- это программное средство использует алгоритмы блочного шифрования AES, Serpent и Twofish.

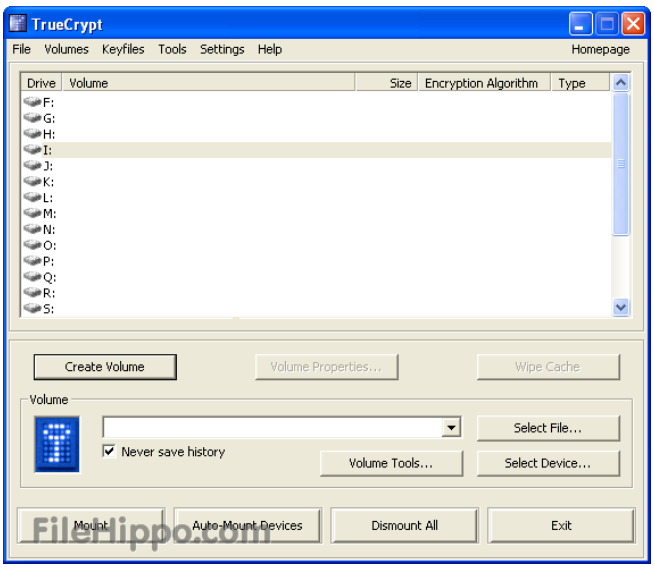


Рис.3.12. **Программное средство TrueCrypt**

Программное шифрование имеет следующие специфики:

- использует компьютерный ресурс одновременно с другими программами для шифрования;
- степень защищенности компьютера определяет степень защищенности носителя;
- пароль, введенный пользователем, используется в качестве ключа шифрования данных;
- может потребоваться обновление программы;
- использование для небольших организаций обеспечивает высокую экономическую эффективность;
- имеется возможность выполнить шифрование для дополнительных методов хранения данных;
- не устойчив к атакам полного выбора пароля или другим атакам, направленным на поиск пароля;
- требует меньших затрат, чем аппаратное шифрование.

Шифрование на уровне диска и файловой системы. *Шифрование диска.* Этот процесс осуществляется для обеспечения конфиденциальности данных, хранящихся на различных носителях (жесткий диск, дискета, USB-накопитель и т.д.). В этом случае каждый бит на всем диске или его части (например, на диске D) шифруется с помощью аппаратного или программного обеспечения для шифрования диска. Целью этого процесса является контроль несанкционированного доступа.

Шифрование всего диска (Full disk encryption (FDE) или *whole disk encryption)* – так называемые средства шифруют все данные на

диске, и только секторы, необходимые для загрузки операционной системы *(master boot record, (MBR))* не шифруются. Некоторые средства шифрования дисков, на основе устройства (Hardware-based full disk encryption, FDE) также шифруют MBR. Они доступны в продуктах следующих производителей дисков:

- *производители жестких дисков:* iStorage Limited, Seagate Technology, Hitachi, Western Digital, Samsung, Toshiba;
- *производители дисков типа SSD:* OCZ, SanDisk, Samsung, Micron, Integral Memory;
- *производители диска USB:* Yubikey или iStorage Limited.

FDE на основе устройства состоит из двух компонентов: средство шифрования на основе устройства и части хранения данных. В настоящее время на практике широко используются три вида FDE:

1. Hard disk drive (HDD) FDE.
2. Enclosed hard disk drive FDE.
3. Bridge and Chipset (BC) FDE.

HDD FDE обычно производятся производителями HDD. При этом производители используют технологию *Opal Storage Specification*. А со стороны Hitachi, Micron, Seagate, Samsung и Toshiba шифрование диска осуществляется с использованием драйвера TCG OPAL SATA.

Некоторые программные средства шифрования дисков используют метод *прозрачного шифрования (Transparent enyptyption)*. Согласно этому методу, после предоставления ключа шифрования все сектора диска автоматически шифруются (включая имя файла, имя каталога, содержимое файла и другие метаданные). К средствам шифрования дисков в виде програмного средства, в качестве примера можно привести *Aloaha Crypt Disk, BestCrypt Volume Encryption, BitArmor DataControl, BitLocker, Bloombase Keyparc, Cryptic Disk, USBCrypt* и других (рис. 3.13).

Метод полного шифрования диска имеет следующие преимущества перед методом шифрования отдельного файла/ каталога:

- почти все пространство замены (swap space) и временные файлы будут зашифрованы. Шифрование этих файлов очень важно потому, что они обычно могут раскрыть важную информацию. Дисковые шифраторы в виде программного обеспечения не шифруют код начальной загрузки (bootstrapping code). Например,

чтобы запустить программное средство BitLocker Drive Encryption оставляется незашифрованная область и полностью шифруются остальные поля;

- этот метод очень полезен, когда пользователь забывает зашифровать закрытые сообщения;

- немедленное уничтожение данных, например, уничтожение криптографического ключа, сделает существующую информацию бесполезной. Рекомендуется физически уничтожить диск, чтобы в будущем избежать возможных методов восстановления данных.

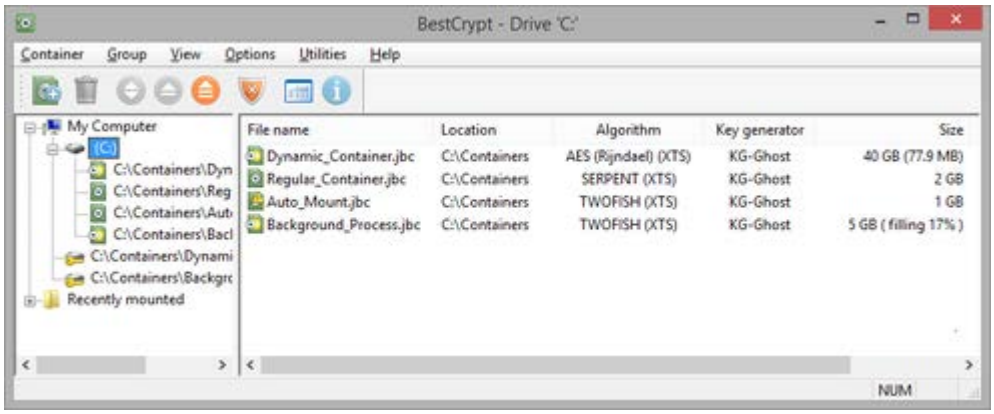


Рис.3.13. **Вид программного средства BestCrypt на ОС Windows**

Шифрование файла (Filesystem-level encryption или *file-based encryption (FBE)* или *file/folder encryption)* – метод шифрования, представляющий собой форму шифрования диска, при которой файлы или каталоги шифруются через файловую систему. Шифрование FBE включает в себя:

- использование криптографической файловой системы, расположенной над основной файловой системой (например, ZFS, EncFS);

- единая файловая система общего назначения, выполняющая шифрование.

Метод шифрования файлов/ каталогов имеет следующие преимущества:

- файловое управление ключами, то есть использование разных ключей для каждого файла;

- отдельное управление зашифрованными файлами проще, чем управление целым зашифрованным диском;

- контроль доступа может осуществляться с использованием криптографических систем с открытым ключом;
- в памяти хранятся только криптографические ключи, а зашифрованные файлы хранятся в открытом состоянии.

3.6. Методы безопасного удаления данных

Безопасное уничтожение так же важно, как и безопасное хранение данных в информационной безопасности. Это связано с тем, что возможность ее восстановления сохраняется в том случае, если конфиденциальная информация не будет полностью уничтожена. Нельзя сказать, что все методы уничтожения данных, которые используются в настоящее время, являются надежными. Ниже можно познакомиться с методами уничтожения документов в бумажном и электронном виде и их характеристиками.

Способы уничтожения документов в бумажном виде. Обычно при уничтожении документов бумажного вида используются следующие методы:

- дробление (шредер);
- сжигание;
- захоронение;
- химическая обработка.

Дробление. С разрешения руководства в организации документы в виде бумаги, находящиеся в руках сотрудников, со временем теряют свою силу или возникает необходимость их уничтожения из-за хранения незначительной информации. Однако в случае дорогостоящих данных в этом случае требуется их полное уничтожение. Процесс дробления является одним из наиболее широко используемых методов при выполнении этой задачи. В этом случае офисный дробильный станок разбивает бумагу, разрезая на очень мелкие кусочки (рис. 3.14).

Преимущество метода дробления заключается в следующем:

- купив один раз можно использовать долгое время;
- для уничтожения материалов не требуется дополнительного пространства;
- может также измельчать конфиденциальную информацию.

Рис. 3.14. **Шредер Rexel Auto+ 90X**

Сжигание. С помощью сжигания можно быстро уничтожать большие объемы документов. С экологической стороны этот метод уничтожения данных не одобряется. Кроме того, метод сжигания имеет следующие недостатки:

- требуется специальное место для сжигания бумаг внутри или за пределами организации;
- если сжигание не осуществляется в специальных котлах в повышенных условиях, то существует вероятность того, что плотно спрессованные папки не будут полностью сожжены;
- разведение огня, погрузка и разгрузка документов требует дополнительных затрат.

Захоронение. Хотя раньше этот метод широко применялся, в настоящее время он используется редко. Этот метод не дает возможности полностью уничтожить данные на бумаге. В регионах с сухим климатом, требуется много времени, чтобы информация на бумаге исчезла.

Химическая обработка. Вышеуказанные методы не дают полной гарантии при уничтожении документов с высоким уровнем конфиденциальности. А химический метод позволяет стирать информацию в виде бумаги со 100% уверенностью. Для этого используется специальное химическое вещество и вода. Восстановить образовавшуюся массу вообще невозможно. Единственным недостатком этого метода является высокая стоимость и необходимость специального места.

Уничтожение электронных документов. Проблема доверия к электронным средствам массовой информации становится все более актуальной в связи с ростом количества способов незаконного использования личной и организационной информации, хранящейся в электронном виде. Например, Агент национальной безопасности США Эдвард Сноуден в начале июня

2013 года раскрыл соответствующие документы организации NSA. Согласно им, говорилось, что за саммитом G20, в том числе за Дмитрием Медведевым следят американские и британские разведслужбы. Секретные агенты с помощью программы PRISM смогли воспользоваться личными данными, хранящимися в ноутбуках или телефонах. Сотрудники правительственного центра связи Великобритании, взломав BlackBerry, получили возможность прослушивания звонков, и читать переписки участников саммита.

Самый легкий путь избавления от информации, содержащейся в электронных средствах, отправка их в *Корзину*, или еще радикальнее – *форматирование.* Хотя большинство пользователей считают этот метод надежным, в реальности все совсем не так. Этот метод обеспечивает физическую потерю данных. В этом случае, есть возможность с помощью специальных программ (Recuva, Wise Data Recovery, PC Inspector File Recovery, EaseUS Data Recovery Wizard Free, TestDisk and PhotoRec, Stellar Data Recovery) восстановить их.

На сегодняшний день на практике в качестве носителей электронных документов используются следующие средства:

- жесткие диски: жесткие диски на компьютере и ноутбуке;
- магнитные ленты (в резервном копировании);
- флоппи-диск: 3.5 и 5.25 дюймовые и др.;
- ZIP диски;
- оптические диски: CD, DVD, Blue Ray и HD DVD;
- флеш памяти и др.

Со стороны правительства Соединенных Штатов разработан ряд нормативных документов по хранению и уничтожению конфиденциальной информации (Code of Federal Regulations). Например, в центрах центрального архива США используются следующие три метода для уничтожения информации, хранящейся в электронном носителе:

Шредирование. Мощные промышленные дробители могут работать практически со всеми портативными носителями: CD, DVD-дисками, дискетами, магнитными лентами и т.д., в результате дробления их на 25 мм куски (рис. 3.15).

Рис.3.15. **Процесс шредирования**

Размагничивание. Свойства запоминающего устройства, которое помещается внутри специального устройства, изменяются, обеспечивая тем самым нечитабельность. Если выполняется сильное размагничивание, данные стираются из устройства, а само устройство переходит в нейтральное магнитное состояние. Этот метод уничтожения данных используется на жестких дисках и некоторых портативных устройствах (рис. 3.16).

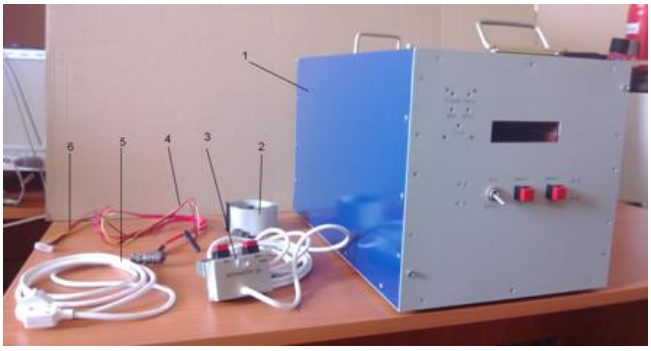


Рис.3.16. **а) Устройство УЭ-02**

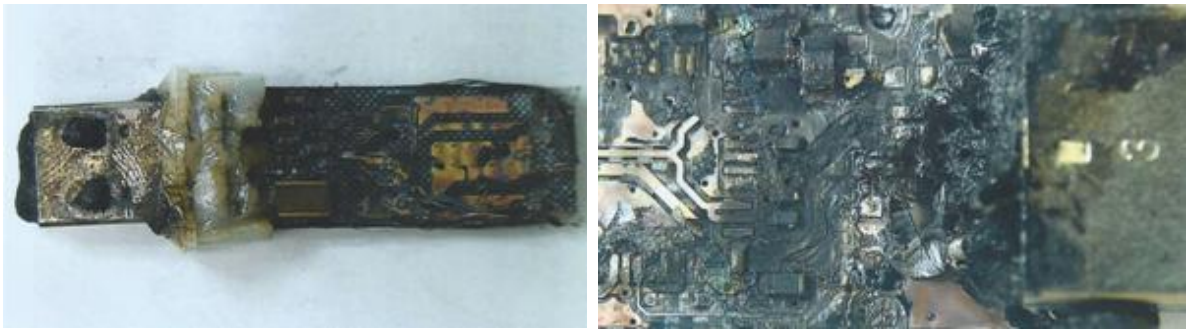


Рис.3.16. **б) Изменение USB флеш накопителя в результате сильного магнитного поля**

Раздавливание. Кроме процесса шредирования в федеральных архивах США существует также метод физического уничтожения жесткого диска путем его раздавливания. Под камнем весом 5,5 тонны будут полностью уничтожены жесткие диски компьютеров и ноутбуков. Этот механизм предназначен для дробления 3.5, 2.5 и 1

дюймовых дисков (SATA, PATA, SCSI), максимальный размер которых составляет 2.5×10×15 см.

Цель описанных выше методов состоит в физическом уничтожении большинства носителей информации. В случае хранения информации, не являющейся TOP SECRET, требуется повторное использование запоминающих устройств. Для этого используются следующие методы:

– повторная запись в запоминающее устройство;

– очистка запоминающего устройства с помощью специальных программ (уничтожение информации перед форматированием).

Хотя этот метод не позволяет гарантированно удалять данные, на практике его достаточно для большинства случаев.

В общем случае при уничтожении информации в электронном запоминающем устройстве используются следующие методы, представленные на рис. 3.17.

Рис.3.17. **Методы уничтожения данных из электронных запоминающих устройств**

Ниже приведены рекомендации Американской компании Cornell по повторному использованию и уничтожению электронных запоминающих устройств (табл. 3.6).

Таблица 3.6

Рекомендации по повторному использованию и уничтожению электронных запоминающих устройств

Электронные запоминающиеся устройства	Для повторного использования	Для уничтожения
Жесткий диск	Удаление перед форматированием с помощью алгоритма DoD 5220.22	Физическое уничтожение или размагничивание
Флоппи диск	Размагничивание или удаление перед форматированием	Физическое уничтожение или размагничивание
Оптические диски	Обычно не применяется	Физическое уничтожение: выравнивание поверхности раздавлением, растиранием
ZIP диски	Удаление с помощью алгоритма DoD 5220.22	Физическое уничтожение или размагничивание
Флеш-запоминающие устройства	Удаление информации перед форматированием	Физическое уничтожение
Магнитные ленты	Размагничивание	Физическое уничтожение или размагничивание

Примечание: Алгоритм DoD 5220.22 основан на уничтожении данных, используемом Министерством обороны США, и предотвращает восстановление данных путем перезаписи до 4-7 раз.

Контрольные вопросы

1. Основные понятия криптографии.
2. В чем разница между расшифровкой и дешифровкой?
3. Преимущества и недостатки шифрования информации с использованием алгоритмов шифрования с симметричным и открытым ключом.
4. Объясните суть принципа Керкгоффа.
5. В чем разница между кодированием и шифрованием?
6. Предметные области криптологии и стеганографии и их различия.
7. Роль симметричной криптографии в защите информации.

8. Роль криптографии с открытым ключом в защите информации.

9. Хэш-функция, требования к ней и ее роль в защите информации.

10. Криптографическое отображение: что такое подмена и замена?

11. Шифрование данных с помощью одноразового блокнота и его безопасность.

12. Симметричные криптосистемы: книга кодов, алгоритмы шифрования A5/1 и TEA.

13. Режимы симметричного блочного шифрования и зачем они нужны?

14. Основные операции модульной арифметики.

15. Алгоритм RSA и математическая проблема, на которой он основан.

16. Методы обеспечения целостности данных.

17. В чем заключаются различия кодов электронной цифровой подписи и аутентификации сообщений и их сходства?

18. Виды средств криптографической защиты информации и их преимущества и недостатки.

19. В чем разница между методами шифрования диска и файла?

20. Методы уничтожения информации на бумаге и их свойства.

21. Методы уничтожения информации на электронном запоминающем устройстве и их свойства.

ГЛАВА 4. КОНТРОЛЬ ДОСТУПА

4.1. Средства идентификации и аутентификации

Понятие *контроль доступа* может использоваться в качестве «зонтика» для решения любой проблемы безопасности, связанной с управлением использования системных ресурсов. Различаются 3 основных понятия: *идентификация, аутентификация* и *авторизация.*

Идентификация – процесс утверждения личности кем-то. Например, можно назвать идентификацией то, что при разговоре по телефону вы представляетесь. При этом вы представляетесь, например, как «Я Баходир». В этом случае вашим *идентификатором* будет «Баходир». *Идентификация* – процесс предоставления идентификатора субъекта системе или запрашивающему объекту. В системе электронной почты, адрес почты называется *идентификатором*, а процесс предоставления адреса называется *идентификацией*. В системе электронной почты почтовый адрес неповторим и уникален. Это означает, что идентификатор пользователя уникален и не повторяется в системе.

Аутентификация – процесс проверки того, что пользователь (или средство, действующее от его имени) имеет право доступа к системе. Например, рассмотрим процесс использования персонального компьютера пользователя. Первоначально пользователь представляет себя (проходит процесс идентификации), предоставляя свой идентификатор (то есть имя пользователя). Затем система запрашивает у пользователя пароль для проверки подлинности предоставленного идентификатора. Если введен соответствующий идентификатору пароль (то есть, аутентифицирован), пользователь получит доступ использования компьютером. В общем случае, аутентификацией называется процесс проверки подлинности пользователя или субъекта.

После аутентификации пользователь получит доступ к системным ресурсам. Однако аутентифицированный пользователь может выполнять только разрешенные действия в системе. Например, допустим, аутентифицированному, имеющему привилегия пользователю требуется предоставление возможности устанавливать программное обеспечение. Каким образом

ограничивается права пользователя, прошедшего аутентификацию? Эта проблема решается путем авторизации.

Авторизация – процесс предоставления права на выполнение действий в системе пользователю, успешно прошедшему процессы идентификации, и аутентификации. В общем случае, аутентификация является бинарным решением, то есть либо разрешается, либо нет. Авторизация – набор правил, используемых для ограничения доступа различных ресурсов системы.

В области безопасности большинство терминов используется также в случаях, отличных от стандартных. В частности, контроль доступа часто используется как синоним авторизации. Однако контроль доступа в этом пособии рассматривается немного шире. То есть процессы аутентификации, и авторизации рассматриваются как отдельные части контроля доступа.

В общем случае из определений, приведенных выше терминов, можно сделать вывод, что:

Идентификация – вы кто?

Аутентификация – действительно ли вы это вы?

Авторизация – вам разрешено делать это?

Односторонняя и двусторонняя аутентификация. Если одна из сторон аутентифицирует другую – *односторонняя,* если обе стороны аутентифицируют друг друга, то это называется *двусторонней аутентификацией*. Например, при использовании электронной почты, только если сервер проверяет подлинность пользователя (с помощью пароля), это называется *односторонней аутентификацией*. В электронных платежных системах сервер аутентифицирует пользователя, а пользователь аутентифицирует сервер. Поэтому данная ситуация называется *двусторонней аутентификацией*.

Многофакторная аутентификация. Во всех описанных выше сценариях аутентификации пользователи проверяются на подлинность только по одному фактору. Например, если при входе в электронную почту вам нужно знать только пароль, то при входе в здание правильный ввод отпечатка пальца будет достаточным, чтобы открыть дверь. То есть сервер требует только то, чтобы у пользователя был правильный пароль или изображение отпечатки пальца. При однофакторной аутентификации, если проверка выполняется только по одному фактору (например, паролю), такая аутентификация называется *однофакторной аутентификацией*.

Идентификация и аутентификация являются первой границей в процессе управления доступом. При реализации системы в разных вариантах некоторые устройства и механизмы могут быть как компонентами подсистемы идентификации, так и аутентификации. Следовательно, следует оценивать средства идентификации, и аутентификации вместе.

Средства идентификации, и аутентификации обычно делятся на три типа в зависимости от факторов аутентификации.

1-й тип. Средства, основанные на знании некоторой секретной информации (например, пароля, секретного ПИН-кода, комбинаций клавиш и фраз) (something you know).

2-й тип. Средства, основанные на использовании уникального устройства, метода или набора данных (например, смарт-карты, цифровые сертификаты) (something you have).

3-й тип. Биометрические средства, основанные на физиологических атрибутах живого организма (something you are), таких как сетчатка глаза, или обычных атрибутах (something you do), таких как подпись.

В некоторых классификациях можно встретить другой тип средств на основе информации, связанной с местонахождением пользователя (some where you are). Поскольку при этом в качестве фактора аутентификации используется номер телефона (страна, город, код района), такие средства часто относят ко 2-му типу (something you have).

Если в системе используются средства, сочетающие разные типы факторов аутентификации, то в этом случае можно говорить о многофакторной аутентификации. Такие системы относят к категории многоуровневой защиты (defence in depth). Поэтому, такие системы более устойчивы, чем системы, в которых используется только один тип устройства. В настоящее время широко распространена двухфакторная аутентификация. Например, современные операционные системы можно настроить с помощью секретного ПИН-кода и смарт-карты.

Парольные системы. Системы, основанные на секретных идентификаторах-паролях (password), являются традиционными средствами аутентификации. К сожалению, парольные системы являются уязвимым по объективным и субъективным причинам.

Во-первых, парольные системы находятся под особым вниманием системных злоумышленников. Злоумышленник может

взломать защиту паролем и, с точки зрения системы, стать авторизованным пользователем. Например, более 80% инцидентов в сфере информационной безопасности связаны со взломом парольной защиты. Большинство компьютерных атак предусматривают именно получение пароля администратора. Следует отметить, что уязвимость многих систем аутентификации связана с их неправильной реализацией. Например, в некоторых системах пароль передается и хранится открыто (с помощью протокола PAP, протокола аутентификации пароля). Протоколы и средства шифрования парольной информации недостаточно криптостойки.

Во-вторых, пароли часто можно просто вычислить. Дело в том, что пароль можно сгенерировать с помощью системы (с помощью датчиков случайных чисел) и, следовательно, его сложно запомнить. В этом случае пользователи часто вводят такие псевдослучайные пароли в лист бумаги, внешнее устройство компьютера, файлы на «рабочем столе», «в памяти» мобильных телефонов и так далее. Это приятная ситуация для злоумышленников.

С другой стороны, легко запоминающийся пароль обычно прост и связан с личной жизнью пользователя и его близких. Следовательно, пароль можно легко найти.

Как можно повысить устойчивость защиты пароля? Есть несколько способов:

- использование одноразовых паролей вместо постоянных (static) паролей;
- усилить политику защиты паролей и учетных записей.

Чтобы исключить риск использования утерянных паролей, используются динамически (dinamic) меняющиеся пароли. Динамические пароли позволяют сгенерировать новый пароль и использовать его по истечении определенного периода времени. Например, если в качестве одного из параметров функции генерации пароля указан день, очевидно, что пароль будет обновляться каждый день. На практике, в качестве динамически меняющихся паролей широко распространены одноразовые пароли (one-time, single –use), применяющиеся за один сеанс работы субъекта.

В системах аутентификации, основанных на динамически меняющихся паролях, клиент и сервер используют один и тот же

алгоритм для генерации паролей. Чтобы контролировать временной интервал действия одноразового пароля, необходимо «синхронизировать» системное время на сервере и на клиенте. Если в контроле пароля используется принцип «начало событий» вместо системного времени, такие системы называются «асинхронными системами».

Усиление политики безопасности парольной защиты предусматривает соблюдение требований, затрудняющих раскрытие пароля при его выборе, а также требований к хранению и передаче пароля по сети, например:

- пароль не должен содержать общих имен, слов, сокращений, дат, номеров телефонов, не соответствовать аутентификатору и т.д.;
- пароль должен содержать заглавные буквы, цифры, знаки препинания и специальные символы (- @ #;% ^ & *);
- количество символов в пароле не должно быть меньше 8, необходимо сменить пароль через 90 дней;
- необходимо установить ограничения на использование учетной записи (по дням, времени суток, адресу подключения, количеству подключений);
- ограничение неудачного ввода пароля и количества попыток - от 3 до 5;
- должны быть установлены режимы криптозащиты для хранения парольной информации, и ее передачи по сети.

Особенными вариантами усиления защиты паролем являются использование парольных фраз (pass phrase) и когнитивных паролей (cognitive – со смыслом). Длинная, но легко запоминающаяся парольная фраза затрудняет раскрытие пароля. Когнитивный пароль обычно состоит из подмножества ответов на случайно выбранные, но тайно заданные вопросы.

Для оценки устойчивости паролей в автоматизированных системах могут использоваться математические показатели. В качестве показателя широко используется информационная энтропия, предложенная Клодом Шенноном:

$$H = n * \log_2|A|,$$

где $|A|$- мощность алфавита пароля (количество возможных символов); n - количество символов в пароле.

Чем больше энтропия, тем сложнее случайное раскрытие пароля. Если пароль находится в словаре выбора пароля, принято, что его энтропия равна нулю.

В заключении следует отметить, что радикальным способом усиления защиты паролем является переход на двухфакторную аутентификацию с использованием дополнительного уникального электронного устройства.

Электронные устройства. Ко второму типу средств идентификации, и аутентификации относятся электронные устройства, которые содержат некоторую уникальную информацию о субъекте. Такие устройства должны быть вместе с пользователем. На рис. 4.1 показана специальная смарт-карта и ее считыватель (считыватель смарт-карт).

Рис.4.1. **Смарт-карта и устройство считывания смарт-карт (ACR39U)**

Электронные устройства можно классифицировать следующим образом:

- по реализации различаются пассивные (только с памятью) и активные (с микропроцессорами) электронные устройства;
- по наличию считывающих устройств различаются электронные устройства с отдельным считывателем (reader), считывающее устройство, интегрированное с ключом (например, подключенное к USB-порту) и электронные устройства, которые используют устройство ввода и основную память компьютера;
- по функциональному назначению различаются статические, синхронно-динамические и асинхронно-динамические электронные устройства.

Статические устройства обеспечивают хранение постоянной уникальной информации и используются для аутентификации или

идентификации субъекта. Простейшим статическим устройством может быть: дискета, карта памяти, бумажная карта с магнитной полосой и АТМ-карта, содержащие, например, идентификатор, пароль, сертификат и т.д.

К современным статическим устройствам относятся:

- смарт-карты – карта размером с кредитную карту, на которую установлен микропроцессор;
- USB-ключи – устройство, которое подключается непосредственно к USB-порту компьютера, содержит микропроцессорный ключ и считывающее устройство;
- электронные таблетки iButton, иногда также называются Touch Memory;
- бесконтактные радиочастотные идентификаторы – радиометки RFID.

Синхронные динамические устройства генерируют пароли через фиксированные промежутки времени. Системное время на сервере и токене необходимо синхронизировать.

Асинхронные динамические устройства генерируют очередной пароль, когда происходит событие (например, когда нажимаются кнопки на сервере и токене). Синхронные и асинхронные устройства могут обеспечивать идентификацию по сгенерированному паролю, а входной ПИН-код или пароль могут обеспечивать аутентификацию. Кроме того, такие системы могут сформировать двухфакторную аутентификацию с помощью имени пользователя.

Устройства с «запрос-ответ» реализуют одноимённый механизм аутентификации. Клиент (ключ) инициирует запрос, сервер, выполняющий функцию аутентификации, генерирует в ответ некоторый псевдослучайный код или фразу и передает назад на ключ. На основе полученных данных электронное устройство вычисляет ответ по установленному алгоритму и отправляет его обратно на сервер. Сервер узнает алгоритм, реализованный в ключе, и выполняет операцию аутентификации, которая проверяет правильность ответа от клиента.

Электронные устройства имеют ряд недостатков:

- устройство может быть нечаянно взломано, если устройство потребляет энергию, необходимо следить за состоянием его источника питания;

- устройство может быть украдено, потеряно, отобрано или использовано кем-либо;
- простые устройства можно клонировать;
- помимо USB-токенов, для большинства устройств, требуется наличие дополнительных считывающих устройств.

Билеты. Идентификацию и аутентификацию можно представить с помощью не только электронных устройств, но и независимого криптографического набора уникальных данных. В сети широко распространены сеансовые билеты или мандаты, предоставляемые участникам во время процесса аутентификации. Примером системы, которая реализует механизм аутентификации с использованием билетов, можно привести Керберос.

Сетевую аутентификацию можно реализовать децентрализовано (на каждой станции) или централизованно. В случае с централизованной реализацией, используется выделенный сервер аутентификации. Популярным сервисом для централизованной аутентификации является Керберос. Его основные особенности:

- при реализации стабильной аутентификации используются сеансовые билеты. Билет содержит зашифрованный секретный ключ, характеристики запроса, временной интервал обмена и т.д.;
- используется симметричный алгоритм для сокрытия аутентификационной информации;
- используются механизмы взаимной аутентификации двух станций (клиента и сервера) до установления связи между компонентами сети;
- в системе реализована технология единого доступа. Это устраняет необходимость для авторизованного пользователя повторно вводить пароль пользователя при выполнении различных сетевых запросов в рамках сессии;
- каждая станция имеет долговременный секретный ключ, хранящийся и на сервере Керберос.

Первоначальный алгоритм аутентификации между клиентом и сервером с участием сервера Керберос выглядит следующим образом:

- клиент отправляет запрос на сервер Керберос, который содержит идентификатор клиента и запрашиваемый сервис сервера;
- Керберос отправляет обратно клиенту сформированный билет, зашифрованный секретным ключом сервера, и копию части

информации из билета, зашифрованную секретным ключом клиента;

- клиент расшифровывает вторую часть билета и отправляет ее вместе с билетом серверу;
- сервер расшифровывает билет и сравнивает его содержимое с дополнительной информацией, отправленной клиентом. Совпадение подтверждает, что клиент и сервер являются уполномоченными абонентами взаимодействия.

Обычно шифрование билета выполняется с использованием симметричных алгоритмов DES, 3DES, AES (Kerberos v5).

Главный недостаток системы Керберос связан с недостатками большинства централизованных систем, в частности, с централизованным хранением секретных ключей в центре распределения ключей (Key Destribution Center, KDC).

Следует отметить, что асимметричное шифрование и электронная цифровая подпись также могут использоваться в протоколах аутентификации.

Биометрические системы. Биометрические устройства основаны на уникальных физиологических или поведенческих (подсознательных) характеристиках живого организма.

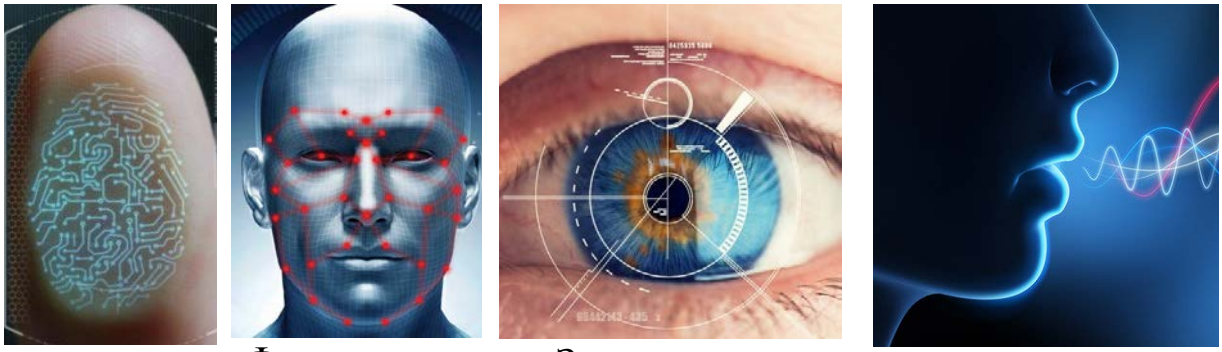
Распространенные биометрические методы включают (рис.4.2):

- по отпечаткам пальцев. Метод сканирования отпечатков пальцев основан на уникальности формы капилляров каждого пальца человека. Сканеры отпечатков пальцев имеют небольшие размеры, универсальны, недороги, широко используются;
- по биометрической форме ладони. Этот метод основан на форме пальцев руки. Эффективность инструментов сканирования ладони можно сравнить с эффективностью сканеров отпечатков пальцев;
- по сетчатке глаз. В этом случае инфракрасный свет направляется через зрачок глаза к кровеносным сосудам его задней стенки. Таким образом, освещенное глазное дно сканируется с помощью специальной камеры;
- по радужной оболочке глаза. Пятно на радужной оболочке – самая уникальная характеристика человека. Преимущество метода в том, что его можно сканировать с расстояния. Это позволяет интегрировать сканеры с камерами наблюдения;
- по форме лица. Метод основан на построении многомерного изображения лица человека;

- по рукописному почерку. Метод основан на графической идентификации подписи или специальной фразы;

- по клавиатурнему почерку. Этот метод обычно основан на особенностях набора предопределенного текста на клавиатуре;

- по голосу. Метод основан на профиле частотных или статистических характеристик человеческой речи. К сожалению, метод зависит от состояния человека.



Отпечаток пальца | Форма лица | Зрачок глаза | Голос

Рис.4.2. **Примеры биометрических образцов**

Идеальный биометрический параметр для использования в области аутентификации должен иметь следующие характеристики:

- *универсальность* – наличие биометрических параметров у всех пользователей;

- *разнообразность* – выбранный биометрический параметр у всех людей отличается друг от друга;

- *неизменность* – выбранный биометрический параметр не меняется со временем;

- *собираемость* – физическое свойство, которое можно легко собрать. На практике накопление физических характеристик также зависит от внимания человека к процессу аутентификации.

Самая надежная из биометрических систем – сканирование сетчатки или радужной оболочки. В настоящее время наибольшей точностью обладают комбинированные устройства, такие как сканеры пяти пальцев и системы, использующие одновременно отпечаток пальца и радужную оболочку глаза.

Существуют следующие особенности и недостатки аутентификации по биометрическим атрибутам:

- биометрика предназначена только для живых организмов;
- из-за вероятностного характера необходимо учитывать чувствительность устройств;
- большинство средств зависят от окружающей среды, возраста и здоровья человека;
- в настоящее время все средства, кроме сканеров отпечатков пальцев, довольно дороги;
- наличие недоверия среди пользователей по поводу угрозы тотального контроля со стороны государства.

С точки зрения потребителя система биометрической аутентификации характеризуется следующими двумя параметрами:
- FAR (False Acceptance Rate) – частота ошибочных разрешений на использование;
- FRR (False Rejection Rate) – частота используемых ошибочных отказов.

Ошибки 1-го и 2-го типа (индикаторы FAR и FRR) взаимосвязаны: чем лучше один параметр, тем хуже другой, т.е. здесь наблюдается обратная зависимость. В идеальной биометрической системе оба параметра ошибок должны быть равны нулю. К сожалению, биометрическая система не идеальна. Поэтому приходится чем-то пожертвовать.

4.2. Логическое управление использованием данных

Контроль доступа. Авторизация – часть контроля доступа для ограничения действий аутентифицированных пользователей, и в большинстве случаев реализуется с помощью моделей контроля доступа.

Управление доступом – определение возможности источника активности объектно-ориентированной деятельности. В целом управление доступом описывается следующей схемой (рис. 4.3):

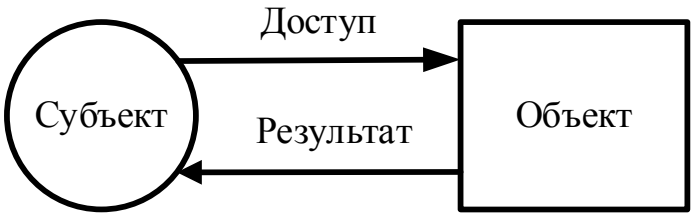


Рис.4.3. **Схема управления доступом**

В настоящее время широко распространены следующие методы управления доступом объектов в системах:

- метод дискреционного управления доступом (Discretionary Access Control, DAC);
- метод мандатного управления доступом (Mandatory access control, MAC);
- метод управления доступом на основе ролей (Role-based access control, RBAC);
- метод управления доступом на основе атрибутов (Attribute-based access control, ABAC).

В системе эти методы не обязательно использовать отдельно друг от друга, то есть можно использовать и их комбинацию.

Метод DAC управления доступом. Этот метод управления доступом применяется для защиты личных активов в системе. В соответствии с этим, владелец объекта сам определяет право пользования им и вид использования.

В DAC управление объектами со стороны субъектов, основано на информации идентификации субъектов. Например, при защите файлов в операционной системе UNIX владелец файла может предоставить остальным одну или несколько операций *чтения (read, r), записи (write, w)* и *выполнения (execute, x)*. В общем случае, метод DAC используется для управления доступом в большинстве операционных систем. Например, на рис. 4.4 показано использование метода DAC в ОС Windows NT/2k/XP.

Однако, серьезной проблемой безопасности DAC является отсутствие полной гарантии того, что он не будет использоваться субъектами, не имеющими доступа к данным. Эта ситуация проявляется, когда любой пользователь, имеющий доступ к данным, имеет возможность отправить их пользователям, не имеющим права использовать данные без разрешения владельца. Кроме того, еще одним недостатком DAC является то, что все объекты в системе принадлежат субъектам, которые определяют их использование. Однако, на практике вся информация в системе принадлежит не отдельным лицам, а всей системе. Наглядный пример этого – информационная система.

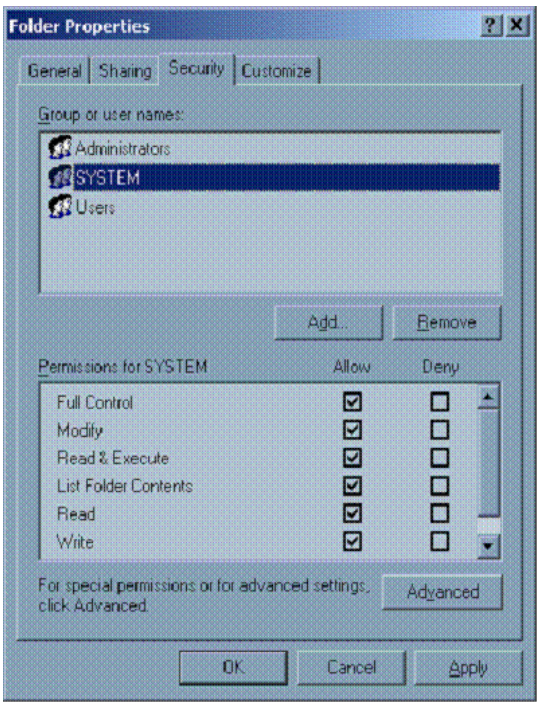


Рис.4.4. **Использование DAC в Windows XP**

В классической системе DAC объект называется «закрытым», если он изначально ни к кому не привязан. Если объект привязан к пользователю и есть ограничения на их использование, он называется «открытым» объектом.

Метод MAC управления доступом. Управление доступом MAC позволяет администратору политики безопасности выполнять управление централизованно. В этом случае пользователь не может изменить политику безопасности. А в методе DAC владелец объекта устанавливает политику безопасности и определяет, кому разрешено ее использовать.

Метод управления доступом MAC позволяет администратору политики безопасности внедрять политику безопасности во всей организации. В методе MAC пользователи не могут случайно или намеренно отменить эту политику. Это позволяет администратору безопасности устанавливать централизованную политику, которая гарантированно применяется для всех пользователей.

Управление доступом в методе MAC основано на классификации субъектов и объектов. Каждый субъект и объект системы будет иметь несколько уровней безопасности. Уровень защищенности объекта характеризуется уровнем важности объекта в организации или размером ущерба, причиненного в случае

утраты. А уровень защищенности субъекта определяется уровнем доверия к нему. Обычно для уровня безопасности назначаются следующие знаки: «*совершенно секретно» (СС), «секретно» (С), «конфиденциально» (К)* и «*открыто» (О)*. Здесь *СС>С>К>О.*

Обеспечение конфиденциальности информации на основе МАС. Если выполняется ряд условий связи между уровнем безопасности объекта и субъекта, то субъект имеет право использовать объект. В частности, должны быть соблюдены следующие условия (рис. 4.5):

- чтение разрешено, если существует уровень безопасности объекта на уровне безопасности субъекта;
- запись разрешена, если уровень безопасности субъекта существует на уровне безопасности объекта.

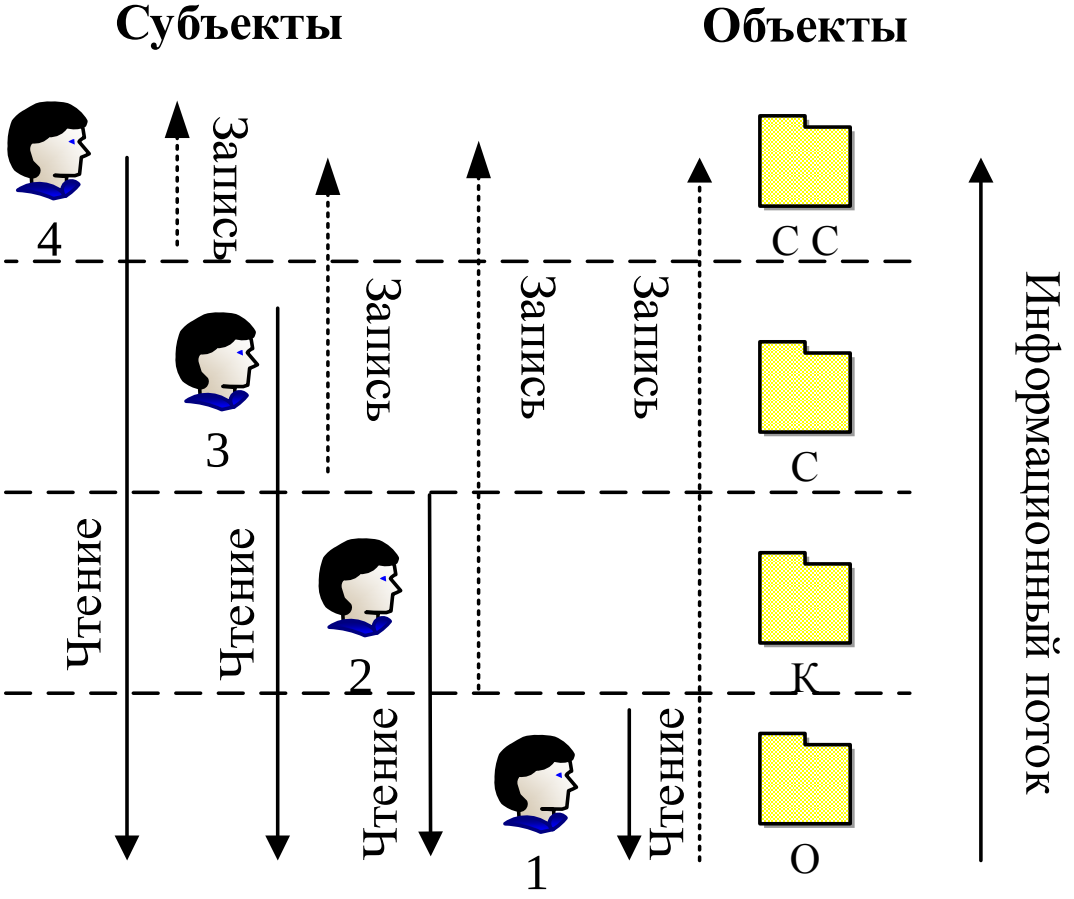


Рис.4.5. **Схема управления информационными потоками для обеспечения информационной безопасности**

В этой модели понятия «пользователь» и «субъект» отличаются друг от друга. В частности, если уровень безопасности присвоен субъекту, пользователь сможет действовать от имени субъекта в то или иное время. Таким образом, в разных случаях один пользователь сможет действовать от имени различных субъектов.

Однако важно, чтобы в какой-то определенный момент пользователь действовал от имени только одного субъекта. Это гарантирует, что информация не передается от верхнего уровня к нижнему.

Есть два неопределенных мнения, которые ставят под сомнение соответствие вышеуказанной модели:

1. Пользователь низкого уровня может писать во все объекты высокого уровня. В этом случае он также может перезаписать существующий объект, что равняется удалению. Этот недостаток можно исправить, запретив запись в высоком уровне. Правила для этой схемы следующие:

- чтение разрешено, если уровень защищенности субъекта включает уровень защищенности объекта;
- запись разрешена, если уровень безопасности субъекта равен уровню безопасности объекта.

2. Как видно из схемы, пользователи с высоким уровнем доверия не могут изменять объекты с низким уровнем безопасности. В преодолении этой проблемы, пользователь может действовать от имени субъектов с разным уровнем доверия, чтобы использовать разные документы. То есть пользователь с уровнем «С» может действовать сам от имени субъекта, доверенного уровня «К» и «О».

Обеспечение надежности информации. Помимо обеспечения конфиденциальности информации, иногда требуется обеспечить надежность информации. То есть, чем выше уровень надежности объекта, тем выше надежность субъекта и чем выше уровень безопасности субъекта, тем более надежные данные он может ввести в систему. Приведенные выше правила для этой модели можно изменить следующим образом:

- запись разрешена, если существует уровень безопасности объекта на уровне безопасности субъекта;
- чтение разрешено, если уровень безопасности субъекта находится на уровне безопасности объекта.

Как видно, случаи, показанные на рис. 4.5, поменялись местами (рис. 4.6). Наряду с использованием уровней безопасности в методе MAC также возможно использовать категории объектов и субъектов. В этом случае, помимо уровня безопасности, может быть предоставлен список категорий, относящихся к каждому объекту и субъекту. Если категории объекта используются для

описания мест, где используется этот объект, то категория субъекта описывает область, в которой он действует. Такая система позволяет более детально управлять доступом.

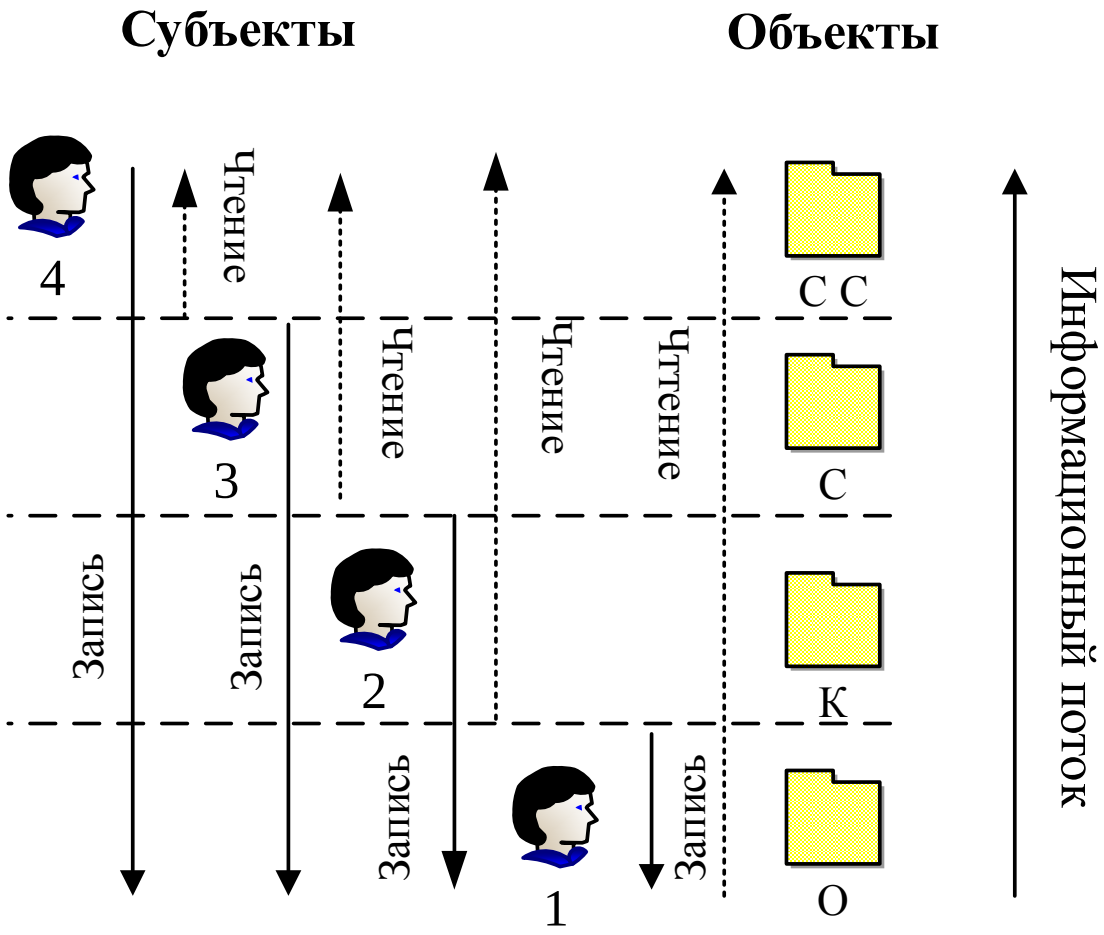


Рис.4.6. **Схема управления информационными потоками для обеспечения надежности данных**

Метод RBAC управления доступом. Основная идея управления доступом в методе RBAC – максимально приблизить принцип работы системы к реальному разделению кадровых функций в организации.

В методе RBAC контроль доступа пользователя к информации основан на типе поведения в системе. Использование этого метода предполагает определение ролей в системе. Понятие роли можно рассматривать как набор действий и обязанностей, связанных с определенным типом деятельности. Таким образом, вместо того, чтобы назначать доступ каждому пользователю для каждого объекта, достаточно указать доступ к объектам для роли. При этом пользователи, в свою очередь, указывают свои роли. Пользователь,

выполняющий роль, будет иметь право доступа, определенный для роли.

В общем, пользователь может выполнять разные роли в разных ситуациях. Иногда одна и та же роль может использоваться несколькими пользователями одновременно. Если в некоторых системах пользователю разрешено выполнять несколько ролей одновременно, то в других может быть ограничение на одну или несколько ролей, которые не конфликтуют друг с другом в любое время.

Основными преимуществами метода RBAC являются:

1. *Простота администрирования.* В классических моделях управления доступом права на выполнение определенных действий с объектом будут зарегистрированы для каждого пользователя или группы пользователей. Ролевая модель предоставляет возможность разделения понятий роли и пользователя на две части: определение роли пользователя и определение доступа к объекту для роли. Такой подход значительно упрощает процесс управления, удаляя старую роль у пользователя при изменении зоны ответственности и назначая роль, соответствующую новой задаче. Если бы право использования было определено напрямую между пользователем и объектами, процедура переназначения новых прав пользователя потребовала бы больших усилий.

2. *Иерархия ролей.* Создав настоящую иерархию ролей, можно создать систему ролей, отражающую реальные бизнес-процессы. У каждой роли могут быть свои привилегии, а также привилегии других ролей. Такой подход значительно упрощает управление системой.

3. *Принцип минимальных привилегий.* Ролевая модель позволяет пользователю зарегистрироваться с наименьшей ролью, позволяя им выполнять необходимые задачи в системе. Пользователи с многочисленными ролями не всегда обязаны использовать все свои привилегии для выполнения определенной задачи.

Принцип минимальных привилегий очень важен для обеспечения надежности данных в системе. Это требует, чтобы пользователю было предоставлено только то, что необходимо для выполнения конкретной задачи среди опций. Для этого требуется определение цели роли, сбор необходимых для ее выполнения привилегий и ограничение привилегий пользователей на этой основе. Отказ в правах пользователя, которые не требуются для

выполнения текущей задачи, защитит систему от нарушений политики безопасности.

4.Разделение ответственности. Еще один важный принцип управления доступом – распределение задачи в системе. На практике достаточно случаев, когда от одного человека не требуется выполнять множество задач, чтобы предотвратить мошенничество. Примером этого является создание человеком платежной информации, и ее подтверждение. Очевидно, что эти действия не могут быть выполнены одним человеком. С другой стороны, ролевой метод помогает решить эту проблему максимально легко.

Официально модель RBAC можно описать следующим образом (рис. 4.7):

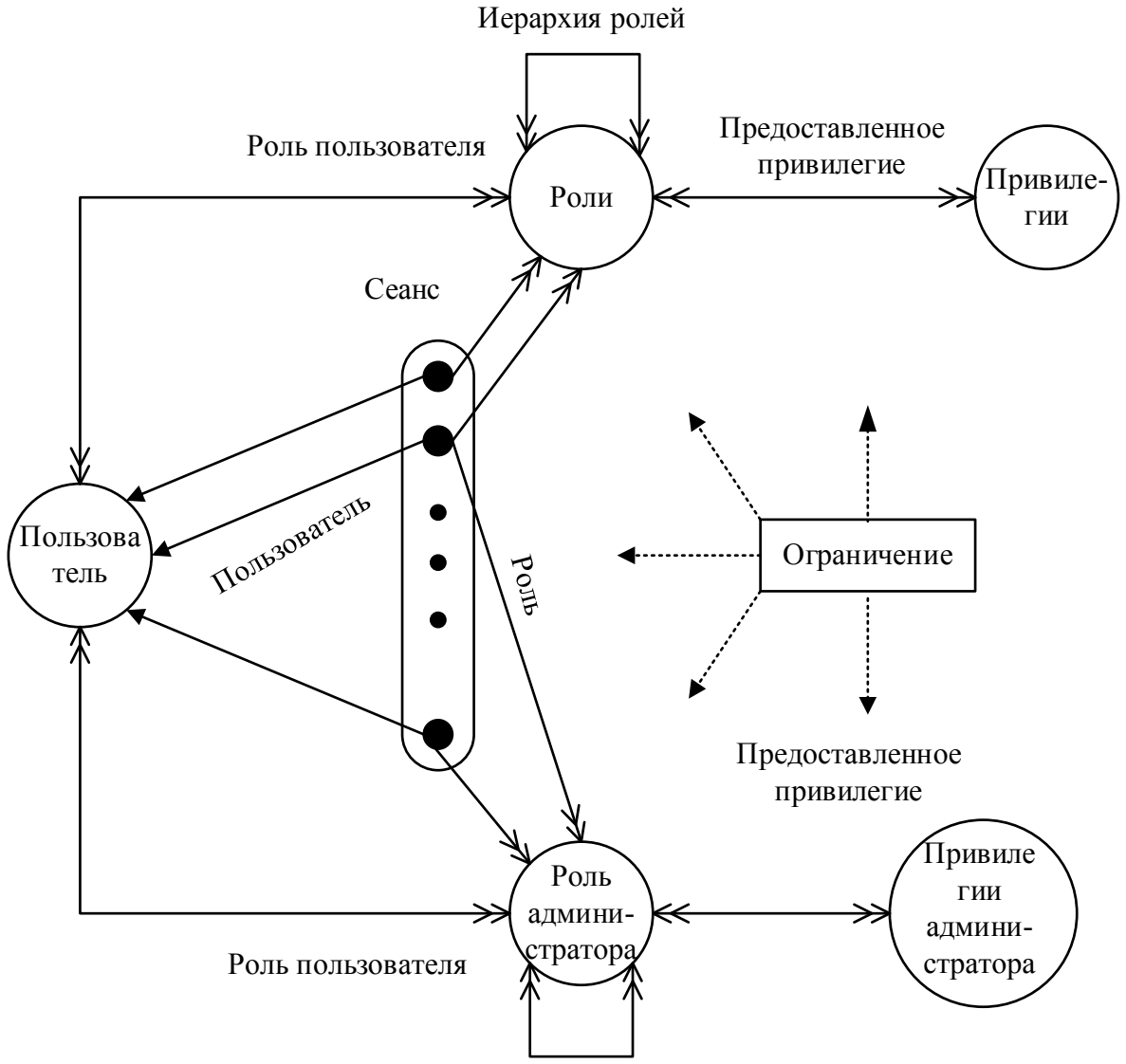


Рис.4.7. **Изображение модели RBAC**

Модель состоит из: пользователей, ролей и привилегий. Пользователь может быть человеком или приложением, действующим от его имени. Если роль – тип деятельности пользователя в организации, привилегия определяется как разрешение на использование одного или нескольких объектов системы. Отношения «назначать роли пользователям» и «назначать привилегии» на рисунке принадлежат ко многим типам. То есть у пользователя может быть несколько ролей, и несколько пользователей могут быть в одной роли. Точно так же несколько привилегий могут принадлежать одной роли, или несколько ролей могут иметь одну привилегию.

Метод ABAC управления доступом. Метод управления доступом на основе атрибутов (ABAC) – управление доступом, основанное на анализе атрибутов объектов и субъектов, возможных действий с ними и правил для среды, соответствующей запросам. В правилах метода можно использовать любой тип атрибута (атрибуты пользователя, атрибуты ресурсов, атрибуты объекта и среды и т.д.). Эта модель основывается на правилах, сформированных с «ЕСЛИ, ТО», состояние о том, кто выполняет запрос, ресурс и действие. Например, ЕСЛИ заявитель является менеджером, ТО должно быть предоставлено право читать/писать конфиденциальную информацию.

Политика на основе атрибутов делает управление доступом более эффективным за счет снижения сложности нормативных требований. Использование политики, основанной именно на этих же атрибутах в разных системах, может помочь управлять соответствием в использовании ресурсов в организации или партнерских организациях. Поскольку такое централизованное управление доступом включает один уполномоченный источник, не требуется, чтобы каждая политика проверяла соответствие определенным системным требованиям.

Одним из основных стандартов для управления доступом на основе атрибутов является XACML *(eXtensible Access Control Markup Language)*, разработанный в 2001 году *организацией* OASIS *(Organization for the Advancement of Structured Information Standards).*

Стандарт XACML содержит следующие основные понятия: правила (rules), политику (policy), алгоритмы объединения правил и политику (rule-combing algorithms), атрибуты (attributes) (субъект,

объект, условия действия и среды), обязательства (obligations) и рекомендации (advices). Правило является центральным элементом и включает в себя цели, воздействия, условия, обязательства и рекомендации. Цель – действия, которые субъект выполняет над объектом (чтение, запись, удаление и т.д.). Эффект основан на логических выражениях, и для доступа к системе может предоставлять одно обоснованное разрешение из следующих состояний: *разрешен, запрещен, невозможно, не определен.* Возврат команды *невозможно* при неправильном логическом условии указывает на наличие *неопределенного* эффекта для ошибок, возникших во время вычисления выражения. Ниже приводится пример метода ABAC.

Цель	Узнайте группу крови пациента из медицинской карты
Действие	Разрешение
Условие	Субъект, должность = Врач & среда, время > = 8:00 & среда, время <= 18:00
Обязательство	Отображение даты регистрации просмотра медицинской карты (среда, время) в журнале

Этот метод управления доступом используется в продуктах Cisco Enterprise Policy Manager, и в Amazon Web Service, OpenStack и т.д.

Матрица управления доступом. Классический вид авторизации начинается с матрицы управления доступом Лампсона. Эта матрица содержит всю информацию, необходимую операционной системе для принятия решения о том, как управлять разными данными для всех пользователей. В этом случае пользователи в операционной системе рассматриваются как *субъекты,* а системные ресурсы как *объекты*. В области авторизации есть два основных понятия: *список управления доступом (Access control list, ACL)* и *список привилегий (Capability list, C-list),* полученные из матрицы управления доступом Лампсона. То есть строки матрицы представляют субъекты, а столбцы представляют объекты. Привилегии, предоставленные определенному субъекту S и объекту O, сохраняются в точке, где их индексы в матрице пересекается. Табл. 4.1 показывает матрицу управления доступом, в которой привилегии представлены в форме привилегий в

операционной системе UNIX, то есть x, r и w представляют собой операции *выполнения, чтения* и *записи*, соответственно.

В приведенной таблице бухгалтерская программа рассматривается как субъект и объект. Это полезный выбор, позволяющий использовать бухгалтерскую информацию только бухгалтерским программным обеспечением. То есть, различные аудиты бухгалтерского учета и балансовая информация должны использоваться только бухгалтерским программным обеспечением, и форма, представленная в матрице выше, обеспечивает это. Однако эта матрица не предотвращает все возможные атаки из-за того, что системный администратор может нарушить эту защиту, заменив программу, принадлежащую бухгалтеру Сэма, на неправильную версию или поддельную версию. Однако этот метод дает Алисе и Бобу право использовать учетную информацию без намеренного или непреднамеренного вмешательства.

Таблица 4.1

Матрица управления доступом

Объект / **Субъект**	**Операционная система**	**Программа отн. бухгалтерии**	**Информация отн. бухгалтерии**	**Информация о страховании**	**Информация о платежном счете**
Боб	rx	rx	p	-	-
Алиса	rx	rx	p	rw	rw
Сем	rwx	rwx	p	rw	rw
Программа отн. бухгалтерии	rx	rx	rw	rw	p

ACL или C-list. Таблица управления доступом состоит из информации, относящейся к решениям об авторизации. Однако, в системе с сотнями (или более) субъектов и тысячами (или более) объектов выполнение операций авторизации с помощью матрицы управления доступом с миллионами (или более) записей создает большую нагрузку на вычислительную систему.

Для оптимального выполнения операций авторизации матрица управления доступом должна быть разделена на управляемые части. Есть два способа разбить матрицу управления доступом. Согласно первому методу матрица делится на столбцы, и каждый столбец хранится с соответствующим объектом. В этом случае, когда запрашивается доступ к объекту, этот столбец матрицы

управления доступом извлекается, и проверяется, что действие разрешено. Эти столбцы можно рассматривать как списки ACL. Например, ACL, относящейся к информации о страховании, в табл.4.1 выглядит следующим образом:

$$(\text{Боб}, -), (\text{Алиса}, rw), (\text{Сем}, rw), (\text{программа, относящаяся бухгалтерии}, rw).$$

Согласно второму способу матрица разбивается на строки, и каждая строка сохраняется с соответствующим субъектом. В этом случае, если субъект пытается выполнить определенное действие, соответствующая строка матрицы управления доступом просматривается, чтобы узнать, разрешено ли выполнение действия. Такой подход называется списком привилегий или C-list. Например, список преимуществ Алисы в табл. 4.1 или C-list равно:

$$(OT, rx), (, \text{программа, относящаяся бухгалтерии}, rx),$$
$$(\text{информация, относящаяся бухгалтерии}, r),$$
$$(\text{данные страховки}, rw), (\text{информация о платежном счете}, rw).$$

Хотя ACL и C-list взаимно эквивалентны, они по-разному хранят одну и ту же информацию. Однако между ними есть незаметная разница. Сравнительный анализ ACL и C-list показан на рис. 4.8.

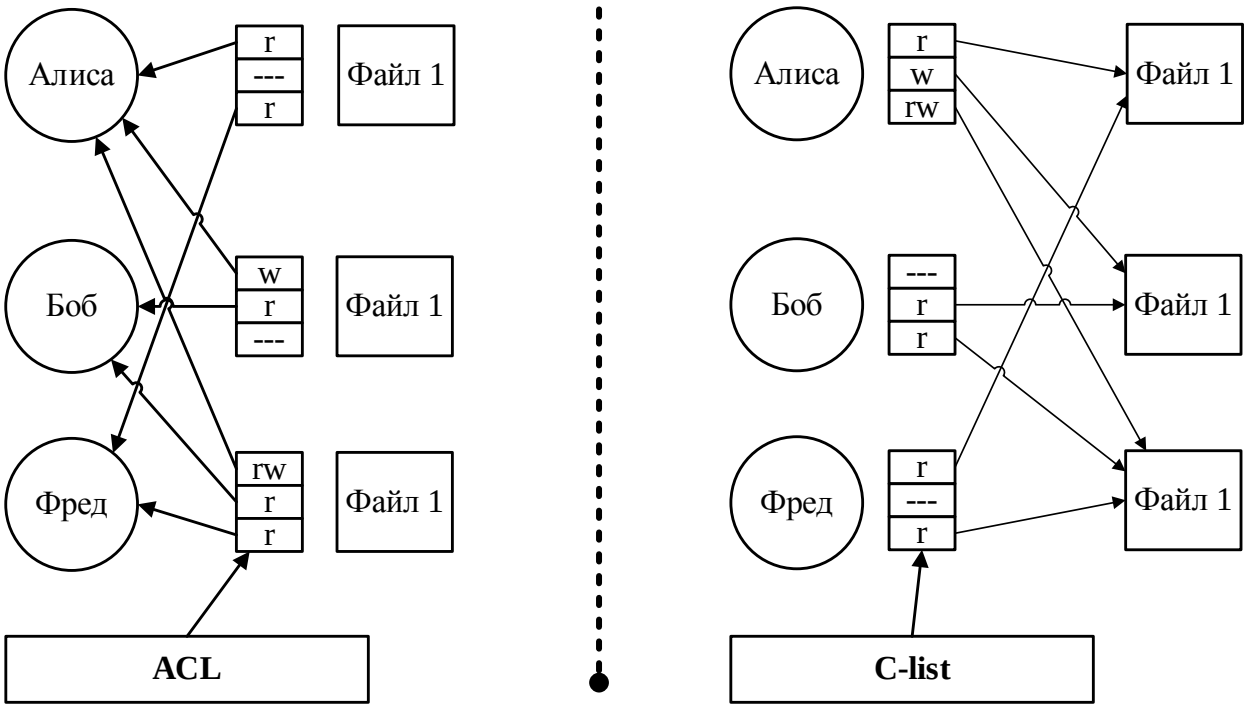


Рис.4.8. **ACL и C-list**

Видно, что показатели на рис. 4.8 имеют противоположные направления, то есть для ACL показатели ориентированы от ресурса к пользователям, а для C-list показатели ориентированы от пользователей к ресурсам. Это, казалось бы, незначительное различие означает, что со списком привилегий (C-list) связь между пользователями и файлами выстраивается внутри системы. Однако в системе на основе ACL C-list имеет ряд преимуществ в плане безопасности по сравнению с ACL, поскольку пользователям требуются отдельные методы для ссылки на файлы, и поэтому по C-list проводилось мало научных исследований.

Беспорядочный помощник – классическая проблема безопасности во многих отношениях. Чтобы пролить свет на эту проблему, была взята система с двумя ресурсами: первый ресурс был компилятором, второй – файлом с именем BILL, содержащим секретную платежную информацию, и одним пользователем, Алисой. В этом случае компилятор имеет возможность писать в любой файл, а Алиса может запускать компилятор. Для этого требуется ввести имя файла, в котором записана информация отладки (процесса поиска ошибок в программе). Однако Алисе не разрешено писать, поскольку это может повредить файл с именем BILL. Матрица управления доступом для этого сценария представлена в табл. 4.2.

Таблица 4.2

Матрица управления доступом для состояния беспорядочного помощника

	Компилятор	**BILL**
Алиса	x	-
Компилятор	rx	rw

Предположим, Алиса запускает компилятор и указывает на BILL в качестве имени файла. Поскольку Алиса не имеет этой привилегии, данный порядок не применяется. Однако, компилятор, работающий от имени Алисы, имеет возможность перезаписать файл BILL. Если компилятор работает с собственными возможностями и запускается Алисой, то он может повредить файл BILL (рис. 4.9).

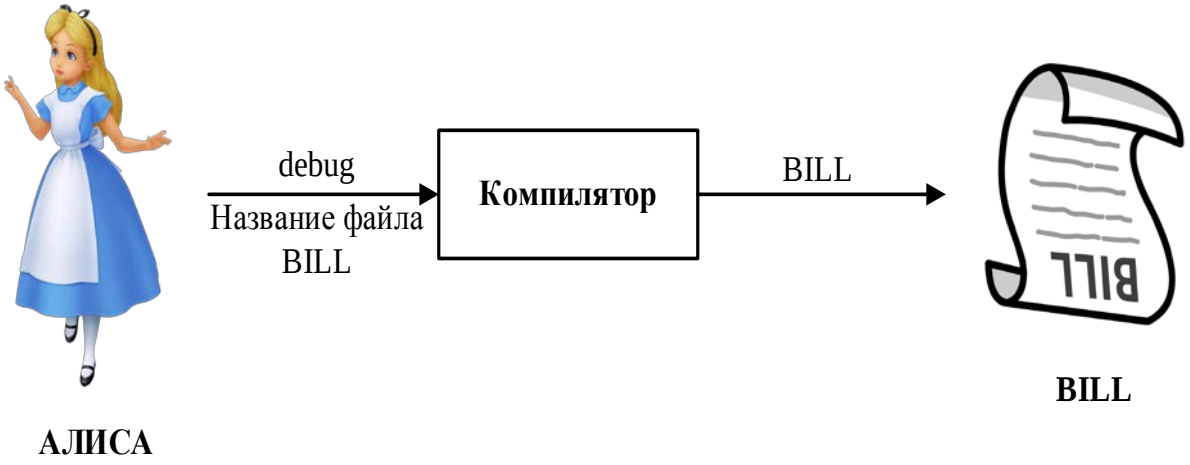


Рис.4.9. **Беспорядочный помощник**

Почему это называется беспорядочным помощником? Поскольку компилятор находится на стороне Алисы и, следовательно, ее помощник, она действует по своему усмотрению, а не по привилегиям Алисы.

Предотвратить это состояние с помощью ACL очень сложно (но возможно). С другой стороны, с помощью C-list может легко устранить это. В системах на основе привилегий, когда Алиса делает запрос компилятору, она выдает ей свой C-list. В этом случае компилятор проверяет C-list Алисы и создает файл отладчика, в случае, когда он имеет привилегию. Поскольку Алисе не разрешено перезаписывать файл BILL, ситуация на рис. 4.9 не наблюдается.

Очень полезно взаимно сравнивать полезные стороны ACL и C-list. ACL обычно предпочтительнее, когда пользователь контролирует свои данные и сосредоточен на защищенной информации. Также легко обмениваться правами на ресурс с помощью ACL. С другой стороны, легко предоставлять полномочия с помощью списка параметров, и пользователю очень легко добавлять или удалять. Благодаря способности предоставлять полномочия можно легко избежать проблем с беспорядочным помощником. Однако реализация возможностей немного сложна и требует больших затрат. Хотя это не совсем понятно, многие проблемы, присущие распределенным системам, возникают с их возможностями. Поэтому ACL в настоящее время используется больше, чем C-list.

4.3. Многоуровневые модели безопасности

Существует множество моделей многоуровневой безопасности (multilevel security, MLC). Ниже можно познакомиться с самыми простыми из них.

Модель Белла-ЛаПадулы. Название Белла-ЛаПадула связано с именами его создателей Белла и ЛаПадулы. Эта модель используется для формализации механизмов управления мандатным доступом с учетом уровня конфиденциальности. Известно, что мандатный принцип ограничения доступа подразумевает наличие иерархических уровней конфиденциальности объектов и соответствующие им метки конфиденциальности.

В модели Белла-ЛаПадулы субъекты и объекты в системе распределяются в соответствии с грифом секретности, и соблюдаются следующие авторские правила:

1. *«Простое правило безопасности» (Simple security).* Согласно этому правилу, субъект имеет право читать информацию только из документов, уровень безопасности которых не превышает его уровень безопасности. Схема информационных потоков, соответствующая реализации этого правила в системе с тремя уровнями секретности, представлена на рис. 4.10.

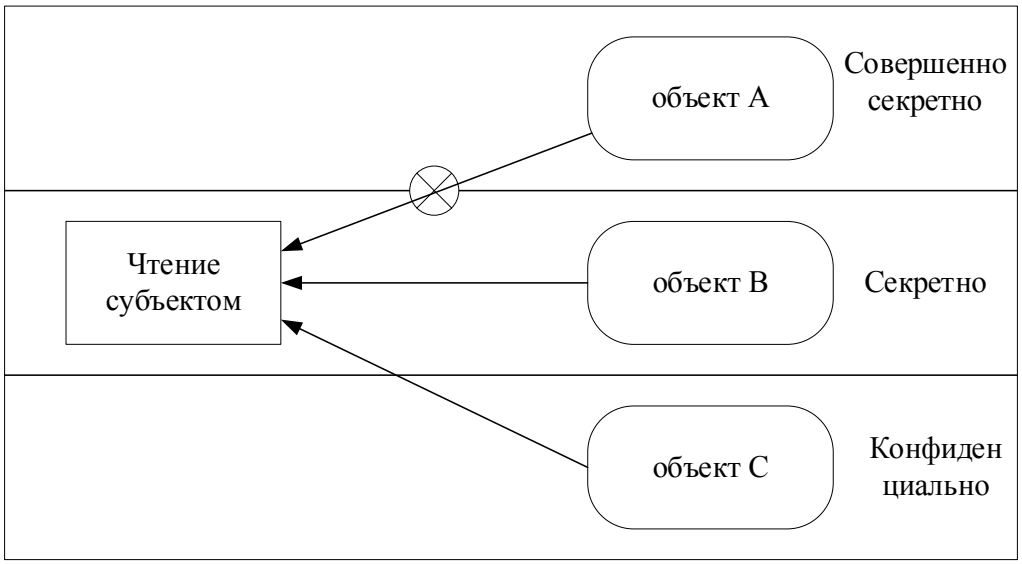


Рис.4.10. **Схеме информационных потоков для свойства «*Simple Security*»**

2. *«-свойство» (-property).* Согласно этому правилу, субъект может вводить информацию в документы, уровень безопасности которых не ниже его уровня безопасности. Схема информационных потоков, соответствующая реализации этого правила в системе с тремя уровнями секретности, представлена на рис. 4.11.

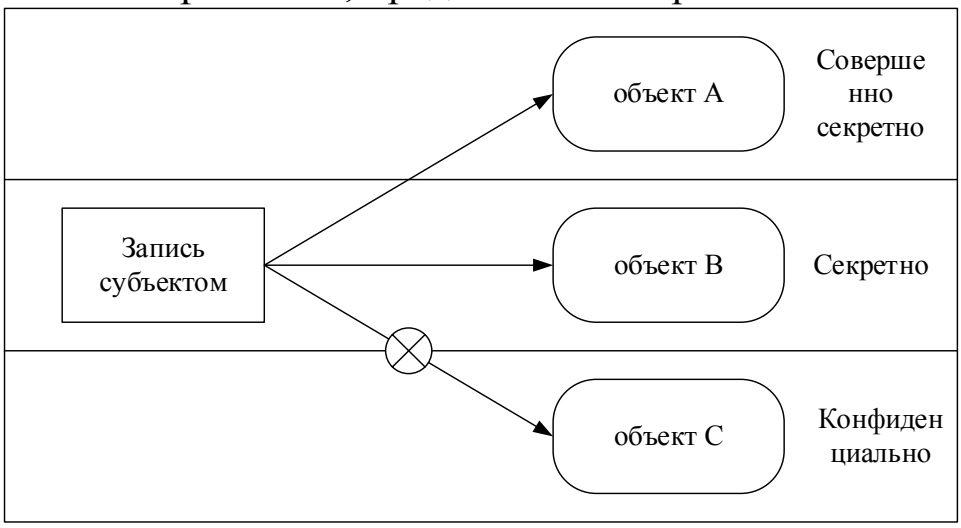


Рис.4.11. **Схема информационных потоков для свойства *«-property»***

3. *«-Строгое свойство» (-Strong Property).* Согласно этому правилу, субъект с правом чтения и записи может выполнять операции только с объектами на своем уровне. Схема информационных потоков, соответствующая реализации этого правила в системе с тремя уровнями секретности, представлена на рис. 4.12.

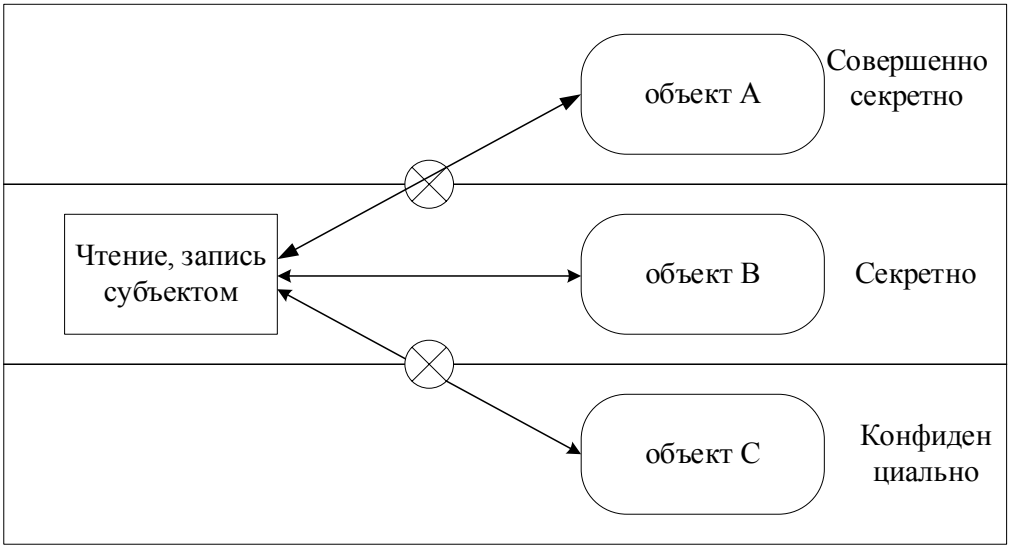


Рис.4.12. **Схема информационных потоков для свойства *« - Strong Property»***

Модель Биба. Эта модель является модификацией модели Белла-Лападулы, ориентированной на обеспечение целостности

данных. Базовые правила модели Биба формулируются следующим образом:

1. *«Простое правило целостности» (Simple Integrity, SI).* Согласно этому правилу, субъект не может читать информацию с уровня целостности, которая ниже своего уровня. Схема информационных потоков, соответствующая реализации этого правила в системе с тремя уровнями целостности, представлена на рис. 4.13.

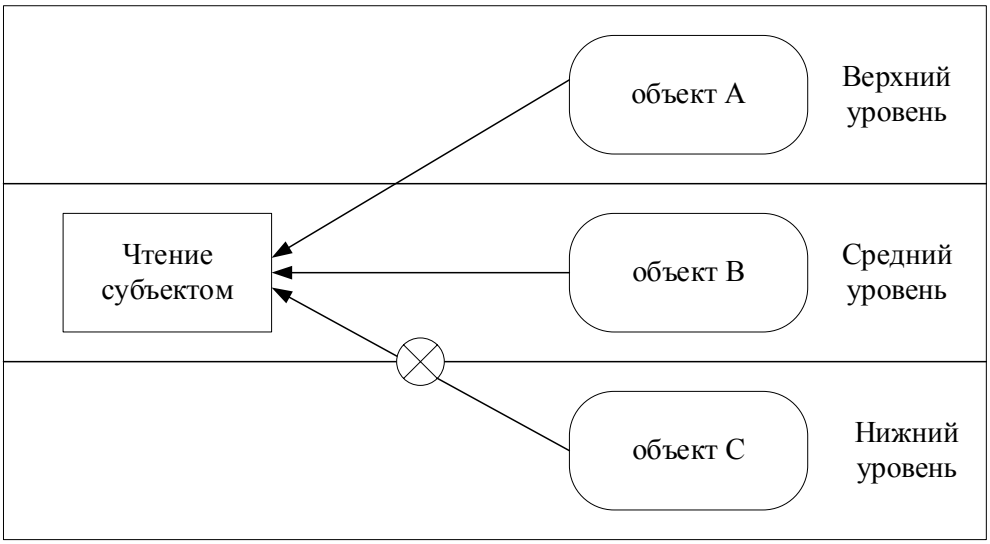


Рис.4.13. **Схема информационных потоков для свойства «*Simple integrity*»**

2. *«Целостность» (-Property).* Согласно этому правилу, объект не может записывать информацию со своего уровня на более высокий уровень целостности. Схема информационных потоков, соответствующая реализации этого правила в системе с тремя уровнями целостности, представлена на рис. 4.14.

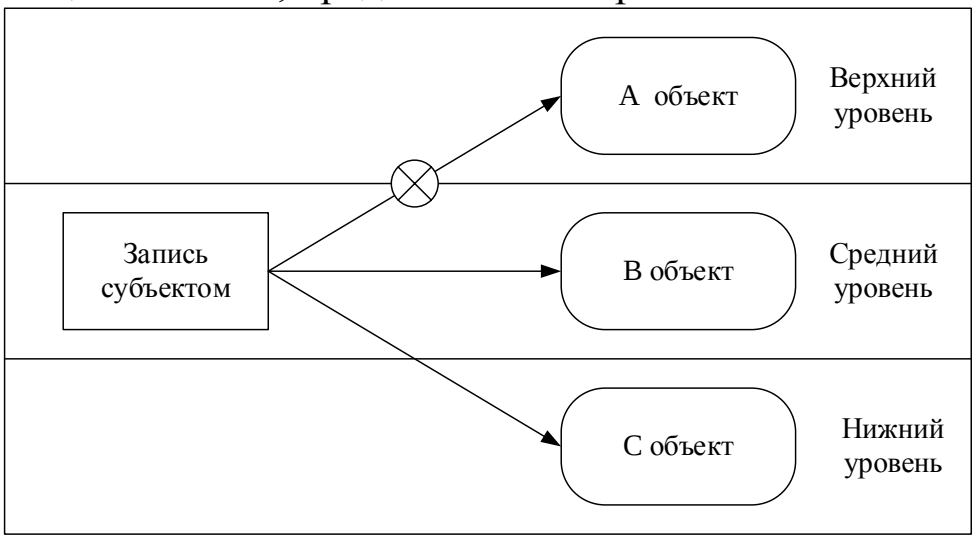


Рис.4.14. **Схема информационных потоков для свойства «*-Property*»**

3. *«Свойство вызова» (Invocation Property).* По этому правилу субъект не может запрашивать сервис у объекта с высоким уровнем целостности.

Следует отметить, что уровни целостности в модели Биба необходимо принимать за уровни достоверности. Соответствующие информационные потоки, с другой стороны, следует рассматривать как передачу информации из более достоверного набора данных в менее достоверный и наоборот.

Управление логическим и физическим доступом. Логические средства для управления доступом используются для мандата, утверждения, авторизации и обязательства в инфраструктуре и системах внутри нее. Эти компоненты применяют меры управления доступом к системам, приложениям, процессам и информации. Данный метод управления доступом также может использоваться в программном обеспечении, операционной системе, базе данных. Управление физическим доступом – механический вид, который можно сравнить с физическим доступом к запираемой комнате. Сам факт разделения логического и физического типа управления доступом является неоднозначным. Например, физический контроль обычно осуществляется с помощью электрических замков, работающих через программы, карточных чипов и программное обеспечение. То есть, в этом контексте физический доступ также можно считать логическим.

4.4. Физическая защита данных

Одним из первых шагов по обеспечению информационной безопасности является *физическая безопасность*. Организации должны находиться в среды соответствующего управления физической безопасностью для предотвращения несанкционированного физического управления, угроз, исходящих от отдельных лиц, и угроз окружающей среде. Системный администратор должен гарантировать, что меры физической безопасности установлены и работают должным образом для защиты от угроз физической безопасности.

Физическая безопасность защищает устройства, людей, сети и данные от атак. Защита данных, сети и устройств, включает защиту от естественных и искусственных (осуществленных со стороны

человека) угроз. Организации должны учитывать все обстоятельства, влияющие на физическую безопасность их инфраструктуры и информационных систем, при использовании соответствующих мер безопасности для обеспечения физической безопасности.

Физическая безопасность – важная часть программы информационной безопасности организации, и в прежние времена люди для обеспечения физической безопасности пользовались ключами, охранниками, шлагбаумами, воротами и т.п. На сегодняшний день форма физической безопасности резко меняется, и от организаций требуется контролировать защиту персонала, активов и недвижимости. Обеспечение физической безопасности этих активов является одной из важных задач для организации, и при проектировании физической безопасности основное внимание уделяется архитектуре здания, оборудованию, рабочей силе, природным явлениям, источнику энергии, контролю температуры и многому другому.

Задача физической безопасности заключается в защите здания и активов организации от краж, вторжений, стихийных бедствий, изменения климата, изменений окружающей среды и человеческих угроз. Многоуровневые меры защиты защищают организацию от различных физических угроз. Первый уровень безопасности контролирует внешний доступ в помещения организации и движение внешних транспортных средств. Этот уровень защиты предотвращает проникновение посторонних или злоумышленников на территорию организации и снижает потенциальные риски для организации на начальном уровне. Следующий уровень защиты защищает автомобили, людей и другие активы организации от внутренних и внешних угроз. На этом уровне обеспечивается бесперебойная электроэнергия, отделение основных зданий организации от парковок, установка хорошо оборудованной водопроводной системы с соответствующей вентиляцией, соответствующими системами сигнализации и т.д. Следующий уровень – важнейшая часть физической защиты, которая контролирует (персонал), входящих извне и изнутри. Если злоумышленник начинает атаку на физический актив, он может получить доступ к секретной информации организации.

Необходимость физической безопасности. Сложность кибератак становится причиной использования злоумышленниками

различных методов взлома физической безопасности организации. Злоумышленники осуществляют свои действия, используя уязвимости в системе физической безопасности организации. Исследование, проведенное Department of Health and Human Services Breach Portal США, показало, что наиболее распространенными инцидентами, связанными с безопасностью в организациях в 2015 году, были попытки нарушения физической безопасности (рис. 4.15).

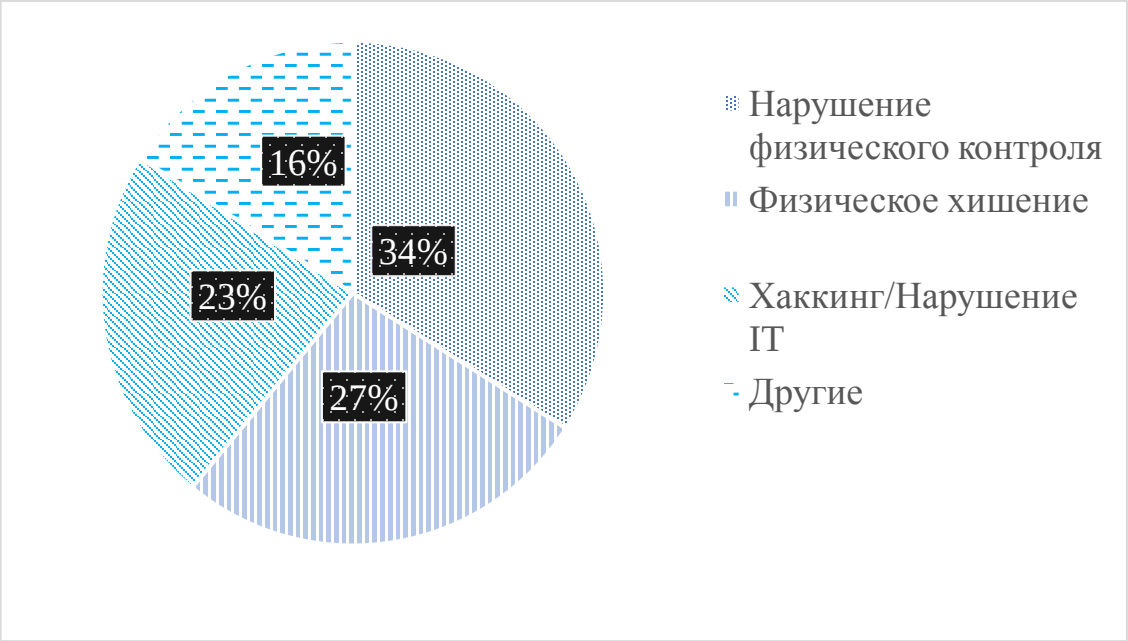


Рис.4.15. **Диаграмма нарушений в соответствии с исследованиями HIPAA (Health Insurance Portability and Accountability Act)**

В отличие от других нарушений безопасности, физические нарушения безопасности могут быть осуществлены без технических знаний в очень редких случаях. Если меры традиционной безопасности, например, межсетевой экран (FireWall), IDS (Instrusion Detection System) и другие средства защиты не обеспечены физической безопасностью, проблемы безопасности возрастут еще больше. Например, межсетевой экран обеспечивает защиту в различных уровнях модели OSI. Однако это не может повлиять на физическую безопасность организации (рис.4.16).

Физическая безопасность обеспечивает защиту на физическом уровне модели OSI. Физический уровень включает:

- все кабельные и сетевые системы;
- физический контроль систем и кабелей;
- электроснабжение систем и кабелей;
- среда поддержки системы.

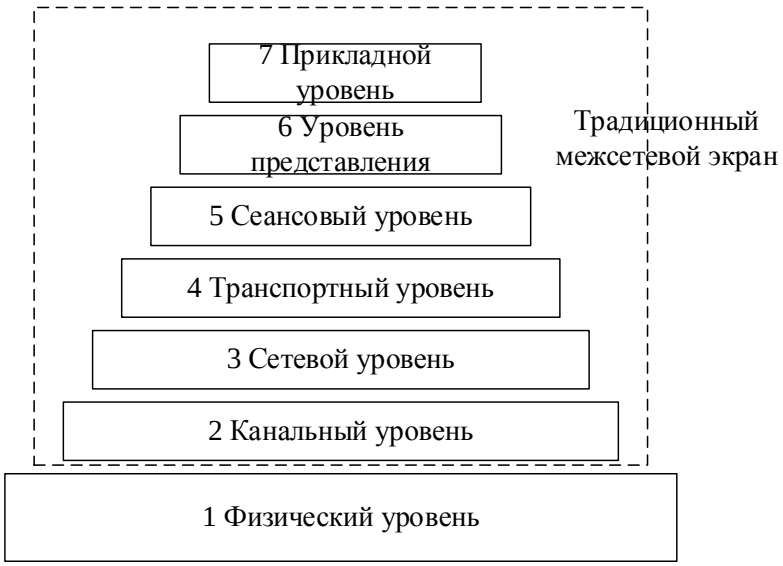


Рис.4.16. **Использование межсетевых экранов на сетевых уровнях**

Факторы, влияющие на физическую безопасность. Факторы, влияющие на нарушения физической безопасности, можно разделить на две группы: *естественные/угрозы информационной среды* и угрозы *со стороны человека (искусственные).*

Естественные угрозы.

Наводнение обычно возникает из-за проливных дождей и таянием льда. Наводнение может повредить электроснабжение организации и серверные помещения. Обычно из-за того, что серверные комнаты в организациях располагаются в подвале зданий, затопление может нанести еще больший ущерб.

Пожары обычно возникают из-за короткого замыкания и старых строительных материалов. Результат пожара может привести к полному или частичному повреждению компьютерных аудиторий и рабочих зданий организации, а также устройств, кабелей и других важных составляющих.

Землетрясение возникает внезапно в результате сильной энергии, которая создает сейсмические колебания в земной коре. Это может повлиять на физическую инфраструктуру организации и

нанести серьезный ущерб компьютерам и другим устройствам, и документам, хранящимся в защищенной среде внутри организации.

Молния и гроза возникают в результате изменений в окружающей среде, что приводит к прекращению всех внешних действий. В результате молнии и грозы изменяется электрическая мощность, что влияет на производительность и на части памяти устройств в организации. Кроме того, молния и гром могут вызвать короткое замыкание в кабелях и других системах подключения.

Для нормальной работы вычислительных устройств, требуется, чтобы они находились в определенной *температурной* среде. Компьютерные средства не предназначены для работы при высоких температурах. Хотя компьютерные системы имеют систему охлаждения, высокие внешние температуры могут отрицательно сказаться на их производительности. Электрическое и электронное оборудование в организации подвержено влиянию изменений *влажности*. Высокая влажность может вызвать коррозию, короткое замыкание или серьезно повлиять на магнитные и оптические накопители.

Искусственные угрозы. Большинство негативных последствий для физических компонентов и сети происходит в результате непреднамеренной или преднамеренной ошибки, совершенной людьми. Существуют следующие угрозы, осуществляемые человеком в системе физической безопасности:

Вандализм. Обиженные сотрудники или бывшие сотрудники могут попытаться дискредитировать систему, нарушив или повредив компоненты системы.

Потеря устройства. Несанкционированное использование может привести к потере важной информации или устройства. Если защиты устройства недостаточно, это может привести к его краже.

Нарушение работы физических устройств. Неисправности устройства, такие как неправильное хранение устройств или данных, отказ от замены поврежденных устройств и уязвимые кабели, могут вызвать серьезные повреждения физических устройств.

Воровство. Уязвимости в системе безопасности могут привести к краже оборудования.

Терроризм. Террористические акты рядом с организацией или внутри нее, такие как, взрывы в машине, взрывы личной бомбы или

взрыва бомбы с дистанционным управлением, могут нанести разнообразный ущерб физической безопасности организации.

Социальная инженерия. Социальная инженерия рассматривается, как попытка человека получить личную информацию незаконным путем. Нарушитель получает доход от сотрудников организации с помощью социальной инженерии, путем несанкционированного физического наблюдения.

Несанкционированный контроль систем. Действие обеих пользователей, как внутренних, так и внешних приводит к утечке информации об организации или несанкционированному управлению системой.

Контроль физической безопасности. Без надлежащего контроля безопасности сложно обеспечить физическую безопасность. В зависимости от того, в какой степени осуществляется контроль физической безопасности, его можно классифицировать следующим образом:

- *административный контроль* объединяет человеческий фактор в управлении безопасностью. При построении административного контроля следует учитывать всех сотрудников на разных должностях. Административный контроль основан на ресурсах, которыми может управлять каждый пользователь, включая ограничения управления, процедуры приложения, процедуры реализации учетной записи и соответствующий уровень защиты информационной системы. Он в основном реализует ориентированные на личности методы для управления человеком;

- *физический контроль* занимается предотвращением повреждения физических систем в организациях и охватывает защиту устройств, зданий или любой секретной среды от несанкционированного контроля. Физический контроль служит для защиты устройства от таких угроз, как потеря или кража, случайное повреждение или разрушение, пожар или стихийные бедствия;

- *технический контроль,* как и логический контроль, использует технологии для контроля доступа физических активов или зданий в организации, обычно для контроля доступа в ограниченной зоне он использует компьютерные устройства, программы, операции и приложения;

- *контроль физической безопасности, расположение и архитектура.* Прежде чем покупать или арендовать помещение для организации следует: учитывать расположение здания, соседние

здания; источники электричества и воды, канализационную систему; близость к малым и крупным дорогам, транспортные проблемы; местонахождение машины скорой помощи, близость к больнице, аэропорту; уровень преступности в районе или различные инциденты безопасности – они должны учитывать все факторы, которые могут повлиять на доступность и другую физическую безопасность. Выбранная территория рекомендуется быть свободной от стихийных бедствий, таких как наводнения, торнадо, землетрясения, ураганы, пожары.

Имея достаточную информацию о расположении зданий, организация должна подготовить список всех активов в здании во время проектирования и планирования внутренней структуры и архитектуры.

При проектировании инфраструктуры и архитектуры организации следует обращать внимание на следующие аспекты:

- на количество входных дверей в здание, парадный вход, лестницы, лифты, парковочные места, проходы и приемные;
- на то, что было проведено собеседование с владельцами и управляющими зданий, чтобы узнать больше о внутренней и внешней архитектуре соседних зданий и прилегающих территорий;
- на угрозы, которые могут нанести ущерб в результате катастрофических сбоев и появления активов извне;
- на изученность влияния на ваши личные данные и важные активы при использовании здания в партнерстве с другими организациями;
- на определение критически важной инфраструктуры, необходимой для обеспечения физической безопасности, хранения конфиденциальной информации и контроля, за эффективной организацией деятельности организации.

Контроль физической безопасности: противопожарные системы. Противопожарные системы объединяют *активную* и *пассивную противопожарную защиту*, которая является важным фактором в обеспечении физической безопасности, определяющим возникновение пожара автоматизированным или неавтоматизированным способом (рис. 4.17).

Рис.4.17. **Оборудования противопожарной защиты**

Средства *активной защиты от пожара* обычно устанавливаются в коммерческих, промышленных и купецких зданиях для предупреждения о пожаре в организации. Основная цель этого метода защиты – предотвратить распространение огня на другие части здания, и требуется выполнение определенных мер автоматизированным или неавтоматизированным способом.

Система активной защиты от пожара включает в себя системы распыления воды, дыма/пожарной сигнализации, системы пожаротушения и различные системы распыления жидкости (спрея).

Системы активного пожаротушения включают в себя:

- система *обнаружения пожара* включает в себя *датчики дыма, датчики пламени* и *тепловые датчики,* которые помогают обнаруживать пожар до распространения огня.

- *системы предотвращения пожара* предотвращают пожары на ранних стадиях без вмешательства человека, уменьшают повреждения и защищают оборудование от разрушения. Системы предотвращения пожара делятся на автоматизированные и неавтоматизированные. Примерами таких систем являются *огнетушители и системы распыления воды*.

Противопожарные пассивные системы защиты рассматриваются как защитные меры противопожарных дверей, окон и стен, предотвращающие распространение огня по всему зданию, не требующие ввода в эксплуатацию какой-либо другой системы.

На практике эти системы реализуются следующими способами:

- минимальное использование легковоспламеняющихся материалов;

- строительство дополнительных этажей или помещений для предотвращения распространения огня в здании;
- ознакомление пользователей здания с работами, которые необходимо выполнить в случае пожара;
- надлежащая поддержка систем пожаротушения;
- обеспечение наличия достаточного количества запасных выходов.

Контроль физической безопасности: физические барьеры. Обеспечение физической безопасности обычно предотвращает несанкционированное использование в организации путем отделения физической границы от общей зоны до зоны ограниченного доступа с помощью различных физических барьеров. Барьеры можно разделить на *внешние, средние* и *внутренние*, в зависимости от расположения. К внешним барьерам обычно относятся *канавы, стены* и т.д. Средние барьеры обычно используются для предотвращения несанкционированного входа толпы и людей. Внутренние барьеры включают двери, окна, решетки, окна, шторы и многое другое (рис. 4.18).

а) Электрические барьеры

б) Металлические барьеры

в) Тумбы

г) Турникет

Рис.4.18. **Примеры барьеров**

В помещении используются следующие типы физических барьеров:

- *стены/ электрические стены/ металлические барьеры* обычно используются для обозначения зон ограниченного доступа, контролируемых зон и защиты от несанкционированного доступа. Основная цель реализации физических преград:
- заблокировать и задержать злоумышленника;
- определение границ организации;
- защита безопасной зоны от внешних атак;
- защита въезда транспортных средств;

- защита от диверсионных атак.

- *тумба имеет* небольшую вертикальную форму и защищает въезд автомобилей;

- *турникеты* позволяют одному человеку войти внутрь помещения или выйти из него, посредством предъявления им подходящей монеты, билета, отпечатка пальца или жетона;

- *различные двери, окна, решетки, оконные шторы* также используются при организации физической защиты.

Контроль физической безопасности: сотрудник безопасности (охрана) выполняет функции организации, мониторинга и поддержки физической безопасности организации, и отвечает за установку, оценку и разработку системы безопасности для защиты от потери, кражи и неправомерного использования конфиденциальной информации. Высококвалифицированный и опытный сотрудник играет важную роль в безопасности любой организации. Защита, осуществляемая работниками в организации, должна осуществляться в порядке 24x7x365. К лицам, участвующим в обеспечении физической безопасности, относятся:

Охранники обычно несут ответственность за контроль за въезжающими и персоналом через главные входные двери и ворота, в частности, они обязаны следить за тем, чтобы посторонние не проникали на территорию организации и не приносили запрещенные предметы. Ситуация на всех входных воротах в организации контролируется охранниками с помощью камер CCTV (Closed-circuit television) и фиксируется и хранится в определенное время.

Начальник охраны в организации. Начальник охраны в организации отвечает за наблюдение действиями охранников, помощь охранникам при необходимости, разгон толпы, управление замками в здании, системами освещения.

Сотрудник безопасности должен установить, управлять и гарантировать, что связанное с безопасностью оборудование в организации работает должным образом.

Руководитель службы информационной безопасности (Chief Information Security Officer). За последние года, руководитель службы информационной безопасности нес ответственность за контроль всех процессов, связанных с безопасностью в организации, также за сеть и систем безопасности. В настоящее

время требуется, чтобы эти люди обладали техническими знаниями и навыками.

Контроль доступа: методы аутентификации. Задача аутентификации лиц внутри организации также может выполняться турникетами, выступающими в качестве промежуточных барьеров, или охранниками.

Контроль физической безопасности: физические замки используются для ограничения несанкционированного физического доступа. Каждая организация должна выбирать их на основе своих требований безопасности. На практике широко используются следующие типы физических замков:

Механические замки: это самый простой способ ограничить физический доступ в организации, они могут быть с ключом или без ключа. Примеры механических замков приведены на рис. 4.19.

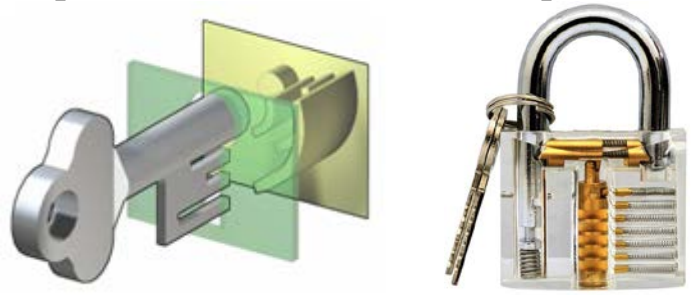


Рис.4.19. **Механические замки**

Цифровые замки: чтобы открыть двери с цифровым замком не требуется ничего (ключ) носить с собой, легко использовать отпечаток пальца, смарт-карту или ПИН-код.

Электрические/ электромагнитные замки: электрическая или электронная система запирания основана на снижении электроэнергии, в результате чего дверь открывается. Обычно они активируются и деактивируются магнитным или электродвигателем. Для открытия этих замков ключ не требуется.

Комбинационные замки требуют ввода секретного кода, состоящего из комбинации цифр и символов.

Контроль физической безопасности: устройство для обнаружения спрятанного оружия/ устройств контрабанды. Организации обычно обнаруживают оборудование или инструменты, различное оружие или контрабандные устройства, бомбы или огнестрельное оружие, принесенные отдельными лицами с помощью специальных сканеров. В качестве примера к таким сканерам можно привести металлодетекторы, системы

обнаружения X-ray и системы обнаружения металла по периметру (рис. 4.20).

Рис.4.20. **X-Ray металлодетекторы**

Контроль физической безопасности: ловушка – средство контроля физической безопасности, которое захватывает нарушителя границы и обычно отделяет опасную зону от безопасной зоны. Ловушка представляет собой небольшую зону, основанную на двухдверной механической системе запирания, при которой первая дверь закрывается до открытия второй двери. Идентификация может быть произведена с помощью смарт-карты, ПИН-кода или биометрических методов (рис. 4.21).

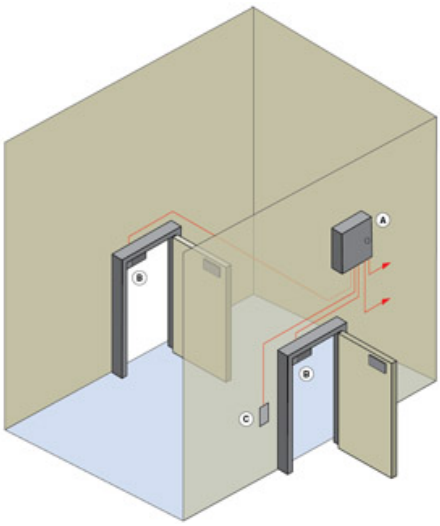


Рис.4.21. **Ловушка**

Контроль физической безопасности: ярлыки безопасности и предупреждающие сигналы. Ярлыки удобны для ограничения разрешений при использовании информации с разным уровнем

безопасности. Для этого данным в организации присваиваются ярлыки безопасности. Доступны следующие ярлыки безопасности:

- открытые данные (unclassified);
- данные с ограниченным доступом (restricted);
- конфиденциальные данные (confidential);
- секретные данные (secret);
- совершенно секретные данные (top secret).

Перед использованием информации, в зависимости от ее ярлыка, определяется, существует ли разрешение или нет, и если разрешено, то можно использовать ее.

Предупреждающие сигналы обычно используются для ограничения несанкционированных действий большого количества сотрудников в организации. К примерам предупреждающих сигналов можно привести такие словосочетания как «ЗАПРЕТНАЯ ЗОНА» (RESTRICTED AREA), «ВНИМАНИЕ» (WARNING) и «ОПАСНО» (DANGER) (рис. 4.22).

Рис.4.22. **Предупреждающие знаки**

Контроль физической безопасности: средства видеонаблюдения являются важным компонентом обеспечения физической безопасности активов организации. Устройства видеонаблюдения обычно устанавливаются у входных дверей, холлов и рабочих зон организации, что помогает контролировать входные и выходные движения. Современные средства видеонаблюдения позволяют не только фиксировать движения, но и обнаруживать нежелательные движения. Например, обнаруживать ситуацию ввоза или вывоза запрещенного устройства или отправлять предупреждающий сигнал при обнаружении конфликтной ситуации. В настоящее время используются в качестве средств видеонаблюдения следующие камеры (рис. 4.23).


а) Dome CCTV б) Bullet CCTV в) C-mount CCTV г) Day/ night CCTV

Рис.4.23. **Камеры наблюдения**

Контроль физической безопасности: политики и процедуры физической безопасности. Каждая организация должна реализовать политику и процедуры физической безопасности, необходимые для обеспечения эффективной физической безопасности. Политики физической безопасности для разных организаций могут различаться. В частности, политика физической безопасности организации включает в себя следующее:

– права и обязанности сотрудников;
– контроль управления доступом;
– регистрация и аудит.

Процедуры физической безопасности включают:

- управление системой запирания;
- регистрация инцидентов проникновения;
- управление посетителями;
- уничтожение конфиденциальных материалов;
- реализация политики *чистого стола* для информации на бумаге и политику *чистого экрана* для обработки информации.

Согласно политике «*чистого стола»*, информация, важная для организации, не должна оставаться без внимания сотрудников и не должна выноситься с рабочего места. А политика *чистого экрана*, направлена на то, чтобы не оставлять сотрудника без присмотра при использовании своего компьютера.

Другие меры физической безопасности: системы освещения. Системы освещения играют важную роль в обеспечении безопасности организационного здания. Недостаточное освещение вокруг здания организации негативно сказывается на эффективности других мер безопасности. Например, если система освещения не соответствует требованиям на входе в организацию,

на автостоянках или в других местах, где установлены камеры видеонаблюдения, шансы обнаружения незаконных действий на этих территориях снижаются. Система освещения окружающей среды делится на следующие в зависимости от состояния и чувствительности:

- *системы постоянного освещения* – осветительные средства, установленные вокруг здания организации;
- *системы освещения в режиме ожидания* – осветительные устройства, которые работают в автоматическом или неавтоматическом режиме под воздействием любого предупреждающего сигнала;
- *мобильные системы освещения* – ручные осветительные средства, которые при необходимости используются для освещения в темноте;
- *системы аварийного освещения* – используются для временного освещения офисных зданий в случае отключения электроэнергии.

Другие меры физической безопасности: источники энергии. Источники энергии оказывают большое влияние не только на систему информационных технологий организации, но и на системы физической безопасности. Недостаточная мощность или частые сбои энергии могут повредить оборудование. Для снижения ущерба от перебоев в подаче электроэнергии в организациях необходимо принять следующие меры безопасности:

- быть готовим к энергетическим колебаниям;
- использование источников бесперебойного питания (UPS – Unintrruptible power supply) в случае отключения электроэнергии;
- установка систем защиты средств от угроз;
- установка систем защиты от статического электричества на рабочем месте;
- правильное использование средств, работающих на электроэнергии.

Безопасность рабочего места: приемная. Приемная организации всегда является важным местом во взаимодействии гостя и организации. Практически каждый день в приемной организации бывают разные гости, партнеры, сотрудники и т.д. Поэтому находящиеся в приемной должны попытаться запомнить и зарегистрировать каждого из них.

Безопасность рабочего места: Безопасность серверов/ устройств резервного копирования. Каждая организация должна уделять внимание физической безопасности своего сервера и средствам резервного копирования. Из-за ограниченного физического доступа к этим средствам они могут использоваться только уполномоченными лицами. Для обеспечения физической безопасности сервера и устройств резервного копирования выполняется следующее:

- хранение сервера и устройств резервного копирования в отдельном помещении. Эта мера ограничивает несанкционированное управление этими устройствами неизвестными лицами или персоналом;
- внедрение камер наблюдения и аутентификации на основе смарт-карты или биометрических параметров в помещении или среде, где расположены сервер и устройства резервного копирования;
- установка серверов на специальные основания для защиты от кражи и повреждения;
- подключение серверов к резервному UPS для защиты от различных изменений энергии;
- хранение устройств в запираемых помещениях;
- обеспечение того, что сотрудники не копируют данные с резервных хранилищ и не выносят серверные средства.

Безопасность рабочего места: важные активы и портативные устройства. Организациям всегда следует обращать внимание на безопасность своего сервера и средств резервного копирования, а также других важных активов, рабочих станций, маршрутизаторов и коммутаторов, принтеров, портативных носителей и т.д. Поскольку все входящие и исходящие данные поступают в организацию через информационную сеть, организация также должна уделять пристальное внимание расположению сетевых кабелей и их безопасности.

Безопасность рабочего места: портативные средства. В настоящее время в каждой организации используются разные портативные средства. Примерами являются ноутбуки, планшеты, проекторы и т.д., которые можно легко украсть, потерять или повредить. Обеспечение физической безопасности этих устройств, требует использования различных механических замков или мер по их хранению в безопасных помещениях (рис. 4.24).

Рис.4.24. **Средство крепления ноутбука к столу**

Контроль среды: системы отопления, вентиляции и охлаждения (Heating, ventilating and air-conditioning system, HVAC). Эти системы используются для управления средой внутри помещения или здания и служат для создания среды, необходимой для работы устройств в организации. Некоторые системы HVAC также имеют систему замораживания, называемую системами HVAC&R (Refrigeration). Они используются не только для создания подходящей рабочей среды для устройств, но также для создания среды, необходимой для работы персонала и организационной деятельности.

Контроль среды: экранирование электромагнитных помех. Электромагнитные помехи от электронных устройств в организации могут повлиять на работу других окружающих устройств. При экранировании электромагнитных помех электронные устройства покрывают металлом, в результате чего резко уменьшается влияние распространяющейся электрической волны на другие среды. Также возможно отделить устройства от других устройств, заслонив их специальными материалами. Когда организации имеют большое количество электронных устройств (например, в телекоммуникациях или больницах), потребность в их экранировании возрастает.

Физическая безопасность: разъяснение/ обучение. Хорошо обученный и квалифицированный сотрудник может минимизировать риски для физической безопасности организации. В целях обеспечения высокой физической безопасности организация должна организовать информационно-разъяснительную работу для своих сотрудников. Программы разъяснения или обучения должны учитывать следующее:

- обеспечение способов уменьшения атак;
- риски хранения секретной информации;
- важность сотрудников службы безопасности;

- оценку вероятности возможных атак на все устройства и данные.

Организации могут использовать различные методы для организации разъяснительных/ учебных курсов по физической безопасности:

- *аудиторные уроки* – преимущества интерактивных аудиторных уроков, основанных на лекции:

- все непонятные и неоднозначные вопросы выявляются на месте;

- проводятся тренинги через веб или на очной основе;

- могут быть более интерактивными с помощью ролевых игр или симуляторов.

- *занятия за круглым столом* – эти курсы обычно проводятся ежемесячно или еженедельно и проводятся для обучения персонала организации, когда требуется физическая безопасность;

- *веб-сайт, информирующий о безопасности* – создав веб-сайт с информацией о безопасности, сотрудники узнают больше о возложенных на них задачах. Текущая ситуация объясняется в нем на основе различных изображений, видео и примеров;

- *уроки мастер-классы* – смена пароля или его удаление без знания пароля выполняется на уроках мастер-классах.

Реализация физической безопасности оценивается с помощью следующих критериев:

1. Установка соответствующих методов контроля доступом для предотвращения несанкционированного доступа.

2. Контроль важных зон на основе правильной системы освещения.

3. Установка и исправность работы системы обнаружения и предупреждения различных угроз, пожара, дыма, электричества, воды и т.д.

4. Правильная установка дверных замков и их правильная работа.

5. Охрана здания и территории организации достаточным количеством охранников.

6. Отправка охранников на учебные занятия.

7. Набор сотрудников службы безопасности из надежных агентств.

8. Правильная установка камеры наблюдения в организации и непрерывная работа.

9. Надлежащее выполнение процедур по обнаружению и регистрации инцидентов, связанных с физической безопасностью.
10. Наличие информации о контакте с персоналом в чрезвычайных ситуациях.

Контрольные вопросы

1. Основные понятия контроля доступа.
2. Каковы методы аутентификации пользователей и их специфические характеристики?
3. Метод аутентификации по паролю, его преимущества и недостатки.
4. Как пароли хранятся в базе данных и методы их сравнения.
5. Что вы понимаете под логическим управлением доступа?
6. Метод управления доступом DAC и его характеристики.
7. Метод управления доступом MAC и его основные характеристики.
8. Метод управления доступом RBAC и его основные характеристики.
9. Метод управления доступом ABAC и его основные характеристики.
10. Объясните понятия ACL и C-list, матрицы управления доступом.
11. Модель Белла-Лападулы и ее основное назначение.
12. Модель Биба и ее основное назначение.
13. Объясните физическую защиту информации, и ее важность.
14. Естественные и искусственные факторы, влияющие на физическую безопасность информации.
15. Способы противопожарной защиты.
16. Роль охранников и камер наблюдения в организации.

ГЛАВА 5. БЕЗОПАСНОСТЬ СЕТЕЙ

5.1. Основные понятия компьютерных сетей

Компьютерные сети состоят из совокупности нескольких компьютеров для обмена ресурсами. Файлы, программы, принтеры, модемы и любое сетевое оборудование могут быть общими или разделяемыми ресурсами. Для объединения компьютеров используются различные средства передачи данных: каналы связи, коммутирующая аппаратура, ретрансляторы и т.д.

Компьютер сети, которому поручено предоставлять различные сетевые ресурсы с помощью соответствующих сетевых служб, называется *сервером*. Сетевые устройства, которые отправляют на сервер запросы в целях доступа к сетевым ресурсам и использования различных сетевых сервисов, называются *клиентами*. Компьютер, работающий автономно или подключенный к сети в качестве клиента, обычно называют *рабочей станцией*.

Компьютерные сети можно классифицировать следующим образом:

- по региональным параметрам;
- по методу администрирования;
- по топологии.

По региональным параметрам различают локальные (LAN, Local Area Network) и глобальные (WAN, Wide Area Network) вычислительные сети.

Локальная вычислительная сеть состоит из компьютерной сети, расположенной на небольшом участке, в комнате или здании. Размер локальной сети зависит от технической архитектуры сети и типа подключения (типа кабеля). Обычно диаметр локальной сети не превышает 2,5 км.

Глобальная вычислительная сеть – регионально распределенная система, которая охватывает большую географическую среду и состоит из множества вычислительных сетей и удаленных компьютеров, связанных магистральными линиями связи. Сети, созданные в пределах мегаполиса и региона, соответственно, называются городской сетью (MAN, Metropolitan Area Network) и региональной сетью (PAN, Personal Area Network).

Самая популярная глобальная сеть – метасеть Интернет, основанная на базе данных стека протоколов TCP/IP. В некоторых публикациях используется выражение «корпоративная сеть». Под этим выражением понимается совокупность нескольких сетей, построенных на разных технических, программных и информационных принципах.

Корпоративную глобальную сеть, использующую для соединения филиалов метасеть Интернет, называют Экстранет (extranet). Корпоративную сеть, реализованную на базе протокола TCP/IP, но изолированную от глобальной сети международного обмена Интернет, называют Интранет.

По способу администрирования сети разделяют на «одноранговые» и «клиент-серверные». В одноранговых сетях все компьютеры могут быть как клиентскими, так и серверными. Примером могут быть UNIX сети.

Сети, построенные по технологии клиент-сервер, имеют специально выделенный сервер. Примеры выделенных серверов: файловый сервер, сервер печати, серверы приложений, серверы регистрации (контроллеры домена), веб-серверы, серверы электронной почты, серверы удаленного доступа, терминальные серверы, телефонные серверы, прокси-серверы и т.д.

В сетях «клиент-сервер» за счет централизованной архитектуры легче обеспечивать функции администрирования и масштабирования сети, безопасности и восстановления. Однако, слабым местом таких сетей (как и всех централизованных систем) является сервер. Сбой сервера может привести к сбою всей системы. Кроме того, для построения сети «клиент-сервер» требуется высокопроизводительный компьютер и соответствующая операционная серверная среда. Соответственно, в таких сетях должен быть профессиональный администратор сети.

По *топологии сети* различают общие шинные (bus), кольцевые (ring), звездообразные (star), сотовые (mesh) и смешанные топологии. Топология *«общая шина»* состоит из сети, проложенной на одной линии. Кабель идет от одного компьютера к другому, а затем к следующему (рис. 5.1).

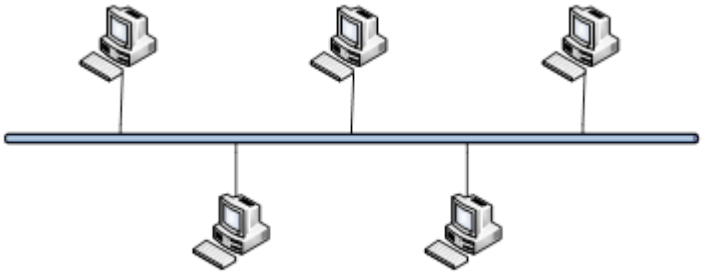


Рис.5.1. **Топология «общая шина»**

На каждом конце шины должен быть терминатор (исключающий отражение сигнала). Один конец шины следует заземлить. Шинная топология считается «пассивной», поскольку компьютеры не регенерируют сигналы. При решении проблемы подавления сигнала используются повторители. Обрыв шины может привести к нарушению работы всей сети (за счет отражения сигнала). Следует отметить, что на физическом уровне система информации слабо защищена. Это связано с тем, что сообщение, отправленное одним компьютером другому, может быть получено на любом другом компьютере.

В «кольцевой» топологии каждый компьютер подключен к двум другим компьютерам, и сигнал распространяется по кругу (рис. 5.2).

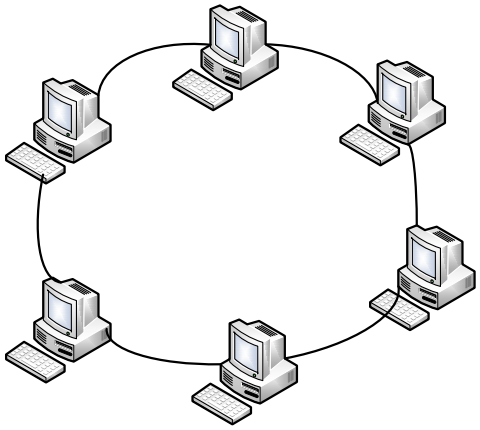


Рис.5.2. **Топология «кольцо»**

Кольцевая топология является «активной», потому что каждый компьютер регенерирует сигнал на следующий компьютер. К недостаткам топологии можно отнести сложность масштабирования и сбой сети в случае прерывания, как в топологии общая шина, а также слабую защищенность информации.

Топология «звезда» создается путем подключения каждого компьютера к центральному концентратору (рис. 5.3).

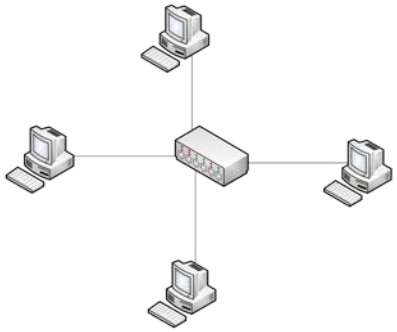


Рис.5.3. **Топология «звезда»**

Преимуществами топологии являются устойчивость сети к разрывам (отключается только один компьютер), возможность добавления компьютеров. К недостаткам топологии относят затраты на концентратор.

В «ячеистой» топологии каждый компьютер подключен к другому. В результате достигается максимальная устойчивость при разрыве соединений. В качестве недостатка топологии можно указать стоимость кабельных соединений.

Следует отметить, что топология может быть физической и логической. Физическая топология подразумевает путь, по которому проложен кабель, а логическая топология – это путь, по которому проходит сигнал. Например, хотя архитектура Token Ring представляет звездную топологию с физической точки зрения, она представляет собой кольцевую топологию с логической точки зрения.

Требования к сети:

- *открытость* – возможность внесения дополнительных абонентских компьютеров и линий (каналов) связи без изменения технических и программных средств существующих компонентов сети;

- *гибкость* – состояние, когда структурные изменения в результате выхода из строя компьютера или линии связи не влияют на работоспособность;

- *эффективность* – обеспечение требуемого качества обслуживания пользователей за счет низких затрат.

Сеть – совокупность разных устройств, следовательно, вопрос их совместного использования является серьезной проблемой.

Прогресс в строительстве различных сетей невозможен без соблюдения производителями общих правил изготовления устройства. Поэтому, достижения в области компьютеров отражаются в стандартах. Другими словами, любая технология имеет «юридическую» защиту только тогда, когда ее содержание отражено в стандартах.

Модель, созданная рядом организаций по стандартизации в начале 1980-х годов, сыграла важную роль в развитии отрасли. Эта модель называется *моделью взаимодействия открытых систем (Open System Interconnection)* или *моделью OSI*. Модель OSI определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень. В соответствии с требованиями этой модели каждая система сети должна быть взаимосвязана путем передачи кадра данных. Согласно модели OSI, генерация и передача кадров выполняется с помощью 7 последовательных действий (рис. 5.4). Эти действия называются «уровнями взаимодействия».

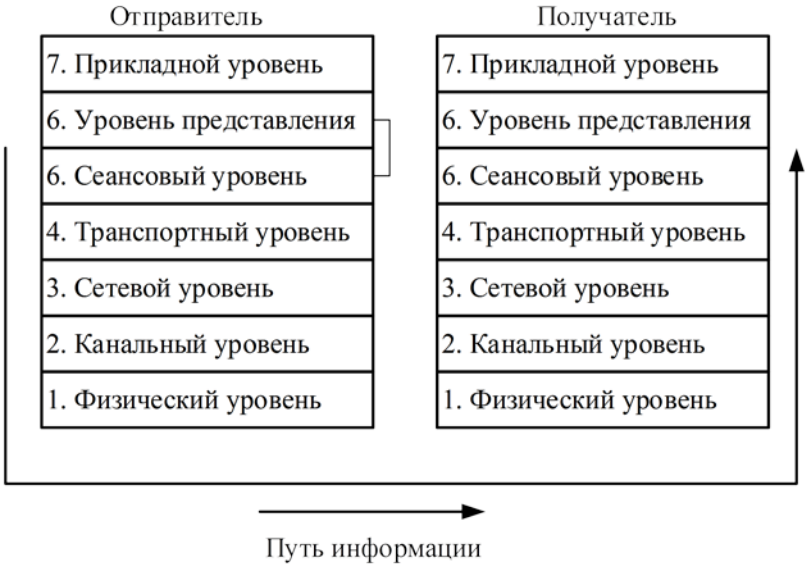


Рис.5.4. **Путь информации от абонента к абоненту согласно модели OSI**

В соответствии с основной идеей этой модели, каждому уровню ставится определенная задача. В результате, вопрос передачи данных разделяется на отдельные вопросы, которые легко можно заметить. В модели OSI средства взаимосвязи разделены на семь уровней: прикладной, представительный, сеансовый,

транспортный, сетевой, канальный и физический. Каждый уровень работает с определенным уровнем связи между сетевыми устройствами.

Итак, пусть приложение обращается с запросом к прикладному уровню, например, к файловой службе. На основании этого запроса программное обеспечение прикладного уровня формирует стандартный формат информации, состоящий из заголовка и поля данных. Заголовок содержит служебную информацию, которую необходимо передать через сеть представительному уровню, чтобы сообщить ему, какую работу надо выполнить. Заголовок, очевидно, должен содержать информацию о месте нахождения файла и о типе операции, которую необходимо над ним выполнить. Как только информация сформирована, прикладной уровень направляет её вниз по стеку представительному уровню. Протокол представительного уровня на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет собственную служебную информацию – заголовок представительного уровня. Полученная информация передаётся вниз сеансовому уровню, который, в свою очередь, добавляет свой заголовок, и т.д. Наконец, информация достигает нижнего, физического уровня, который передаёт её по линиям связи машине адресату. К этому моменту информация «обрастает» заголовками всех уровней. Как только информация достигает машинного адресата, она передаётся наверх по уровням. Каждый уровень анализирует и использует свой собственный заголовок уровня, выполняя задачи, соответствующие этому уровню. Затем он удаляет заголовок и передает информацию на более высокий уровень.

В модели OSI различают два типа протоколов. В протоколах *с установлением соединения* (connection oriented) до обмена информацией, нужно установить соединение отправителя и получателя, и, возможно, следует выбрать некоторые параметры протокола, используемого для обмена информацией. Когда общение закончится, они должны отключиться. Примером взаимодействия на основе соединения является телефон.

Вторая группа протоколов – протоколы без установления предварительного соединения (connection less). Такие протоколы также называются протоколами с *datagramma*. Отправитель передает информацию, когда она готова. Примером связи без

установки предварительного соединения является отпускание письма в почтовый ящик. При взаимодействии компьютеров используются оба типа протоколов.

5.2. Проблемы сетевой безопасности

В области информационной, Интернет и компьютерной безопасности большинство пользователей часто используют понятия угрозы, уязвимости и атаки. Однако есть случаи их замены большинством пользователей.

Уязвимость – недостаток, который может привести к неожиданным и нераскрытым событиям, которые могут поставить под угрозу безопасность системы при «взрыве» или ошибке в проектировании или реализации.

Угроза (угроза информационной безопасности) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Атака – нарушение безопасности информационной системы, позволяющее захватчику управлять операционной средой.

В настоящее время следующие факторы способствуют увеличению количества задач, реализуемых через сеть:

Неправильная настройка устройства или программного средства. Уязвимости в системе безопасности обычно вызваны неправильно настроенным устройством или программным обеспечением в сети. Например, использование протокола, который неправильно настроен или не имеет шифрования, может быть причиной раскрытия секретной информации, передаваемой по сети.

Проектирование сети небезопасным и уязвимым образом. Неправильно и небезопасно спроектированная сеть может столкнуться с различными угрозами и возможностью потери данных. Например, если технологии межсетевого экрана, IDS и виртуальной частной сети (VPN) реализованы небезопасно, они могут сделать сеть уязвимой для различных угроз.

Врожденная технологическая уязвимость. Если устройство или программное средство не может предотвратить определенные типы сетевых атак, оно будет уязвимо для этих атак. Например, если веб-браузер, используемый в системах, не обновлен, он будет более не устойчивым для распределенных атак.

Невнимательность пользователей. Невнимательность пользователей сети может серьезно повлиять на безопасность сети. В результате действий человека могут возникнуть серьезные проблемы безопасности, такие как потеря и утечка данных.

Умышленные действия пользователей. Даже если сотрудник уволен, он все еще может иметь доступ к распределенному диску. В этом случае он может стать причиной утечки конфиденциальной информации в организации. Данная ситуация рассматривается как умышленные действия пользователей.

Виды угроз сетевой безопасности. Сетевые угрозы обычно делятся на два типа (рис. 5.5):

- внутренние угрозы;
- внешние угрозы.

Внутренние угрозы. 80% преступлений, связанных с компьютером или Интернетом, являются внутренними атаками. Эти атаки могут осуществляться изнутри организации обиженными сотрудниками или сотрудниками со злым умыслом. Большинство этих атак осуществляется привилегированными пользователями сети.

Внешние угрозы. Внешние атаки осуществляются в результате уязвимости, уже существующей в сети. Злоумышленник может проводить эти атаки просто ради интереса, материальной выгоды или снижения репутации организации. В этом случае атакующий обладает высокой квалификацией и может проводить атаку в группе.

Внешние угрозы обычно делятся на два типа: *систематизированные* и *несистематизированные* внешние угрозы (рис. 5.5). Систематизированные внешние угрозы осуществляются высококвалифицированными специалистами. Эти люди обладают возможностью быстро идентифицировать существующие уязвимости в сети и использовать их в своих целях. Несистематизированные внешние угрозы обычно реализуются неквалифицированными лицами с помощью различных готовых средств взлома и скриптов (сценариев). Эти типы атак обычно выполняются отдельным лицом, чтобы проверить свои способности или проверить наличие слабых мест в организации.

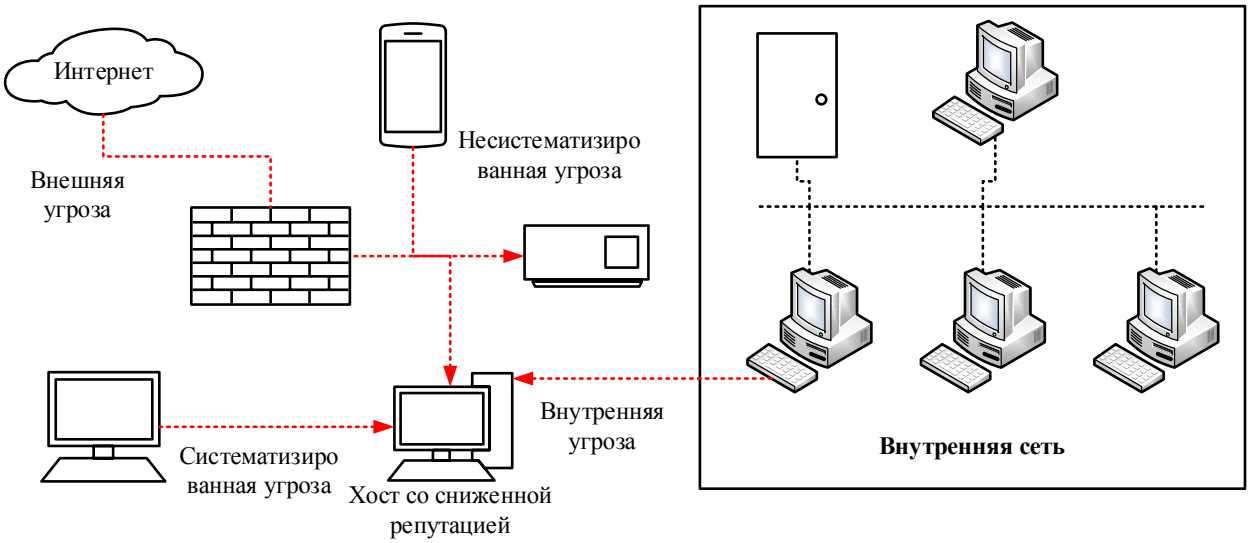


Рис.5.5. **Различные угрозы, направленные на сеть**

По мере увеличения количества атак на сеть организации сталкиваются с проблемами в обеспечении безопасности своих сетей. Кроме того, тот факт, что злоумышленники или хакеры используют все новые способы доступа к сети, разнообразие их мотивов усугубляет эту сложность. Сетевые атаки обычно классифицируются следующим образом:

Разведывательные атаки. Разведывательные атаки собирают информацию об организации и сети с целью простой реализации серьезной атаки, что позволяет злоумышленникам выявлять потенциальные уязвимости, которые могут существовать.

Основной целью разведывательной атаки считается сбор информации, относящейся к следующим категориям:

- о сети;
- о системе;
- об организации.

Существуют следующие типы разведывательных атак:

Активные разведывательные атаки. Активные разведывательные атаки в основном направлены на сканирование портов и операционной системы. Для этого атакующий рассылает разные пакеты с помощью специальных программных средств. Например, специальное программное средство помогает собрать все IP-адреса, которые идут на маршрутизатор и межсетевой экран.

Пассивные разведывательные атаки. Пассивные разведывательные атаки попытаются собрать информацию через трафик. Для этого атакующий использует программное средство,

называемое снифферо́м. Кроме того, атакующий может использовать множество средств.

Входные атаки. Как только будет собрано достаточно информации о предполагаемой сети, атакующий попытается получить доступ к сети, используя различные технологии. То есть он пытается управлять системой или сетью. Эти типы атак называются входными атаками. В качестве примера можно привести несанкционированный доступ, жесткие силовые атаки, повышение привилегий, атака посредника и другое.

Атаки, направленные на пароль. Атаки, направленные на пароль, проводятся с целью получения контроля над компьютерной системой или несанкционированного доступа. Атаки, направленные на пароль, нацелены на кражу секретных данных. Для этого используются различные методы и средства. Ниже перечислены примеры широко распространенных атак:

- атака, основанная на словаре;
- атака грубой силы или атака полного выбора всех вариантов;
- гибридная атака (на основе словарных атак и грубой силы);
- атаки таблицы Rainbow (таблицы, в которых хранятся хэш-значения заранее вычисленных, широко распространенных паролей).

Атака посредника. В атаке посредника (Man in the middle attack, MITM) атакующий проникает в установленную связь и обрывает ее. В этом случае атакующий получит не только информацию, обмениваемую сторонами, но и возможность отправлять фальшивые сообщения. С помощью атаки MITM, атакующий может управлять процессом связи, разговоров или обмена данными в режиме реального времени.

Атаки отказа в обслуживании (Denial of Service, DoS). В атаках, направленных на отказ в обслуживании, атакующий пытается ограничить клиентов, пользователей услугами, доступными в организации. Хотя атаки DoS не приводят к краже или потере какой-либо информации, они приводят к не функционированию организации. Атаки DoS влияют на файлы и другую секретную информацию, хранящуюся в системе, и даже на работу веб-сайта. С этой атакой можно приостановить деятельность веб-сайта.

Распределенные DoS атаки: (Distributed DoS, DDoS). DDoS – атака, направленная на нарушение использования сервиса в

широком спектре целевых систем и сетевых ресурсов, которая осуществляется непосредственно через множество зомби-компьютеров в Интернете. В этом случае сервисы, находящиеся под атакой, рассматриваются как основная цель, а занижение репутации систем (перевод их в состояние зомби) рассматривается как вторичная цель.

Вредоносные атаки. Вредоносные атаки прямо или косвенно влияют на систему или сеть. Вредоносная программа – файл, который имеет возможность угрожать компьютерной системе и может иметь форму троянов, вирусов и «червей».

Вредоносное программное обеспечение – средство, нацеленное на выполнение злонамеренных действий, как и атакующий, без разрешения пользователя, и может быть в форме загружаемого кода (.exe), активного контента, скриптов и т.д. Атакующий может использовать вредоносное программное обеспечение для занижения репутации системы безопасности, нарушения операций компьютера, сбора секретной информации, модификации, удаления или добавления контента на веб-сайт и получения управления над компьютером пользователя. Вредоносная программа также может использоваться для получения больших объемов секретной информации от государственных органов и корпоративных организаций. В настоящее время широко распространены следующие типы вредоносных программ:

- *вирусы:* самоумножающиеся программы, которые прикрепляются к другой программе, загрузочному сектору компьютера или документу;
- *троянские кони:* состоит из скрытого вредоносного кода, но проявляет себя как программное средство, которое на первый взгляд выглядит хорошим и полезным;
- *Adware:* программное обеспечение, отслеживающее деятельность пользователей в маркетинговых целях или для демонстрации рекламы;
- *Spyware:* программный код, собирающий пользовательские данные и отправляющий их атакующему;
- *Rootkits:* эта вредоносная программа скрывает свои действия так, что не обнаруживается со стороны операционной системы;
- *Backdoors:* вредоносные программные коды, позволяющие атакующему обойти систему без аутентификации, например, получить привилегии без пароля администратора;

- *логические бомбы:* вредоносное программное средство, осуществляющее свои действия при выполнении какого-либо логического условия;

- *Ботнет:* компьютеры с заниженной репутацией в Интернете, которые используются атакующим для проведения распределенных атак;

- *Ransomware:* вредоносное программное обеспечение шифрует или блокирует ценные файлы, доступные на компьютере жертвы, и требует оплаты.

5.3. Средства, обеспечивающие сетевую безопасность

В настоящее время к средствам обеспечения сетевой безопасности относят: базовые средства ограничения сетевого доступа (межсетевой экран) и средства защищенной передачи данных (криптошлюзы и VPN - решения), также дополнительные сетевые средства анализа защищенности, средства мониторинга трафика, ложные сетевые цели и т.д.

Межсетевое экранирование. Межсетевой экран (firewall, brandmauer) – базовое средство разграничения сетевого доступа на основе механизма фильтрации трафика. Механизм фильтрации подразумевает проведенные сравнения проходящего трафика с заданными правилами (фильтрами) и принятие решения о пропуске или блокировании сетевых пакетов.

Межсетевые экраны обычно классифицируют относительно используемых технологий фильтрации и базового уровня эталоном модели OSI (табл. 5.1).

Управляемые коммутаторы, функционирующие на канальном уровне, позволяют выполнять функции фильтрации трафика, например, на основании MAC-адресов, портов и других параметров, полученных из заголовков кадров. Достоинством управляемых коммутаторов относят удобство администрирования групп сетевых устройств, повышение производительности локальной сети. Ограниченная функциональность, неудобство физической реконфигурации, и уязвимость к атакам подмены MAC-адреса считаются недостатками управляемых коммутаторов.

Таблица 5.1

Типы межсетевых экранов

Уровень модели OSI	Технологии фильтрации	Тип межсетевых экранов
Прикладной уровень	Прокси	Прикладной посредник
Сеансовый уровень	Прокси	Сеансовый посредник
	Инспекция пакетов	Инспектор состояния
	Фильтрация пакетов	Динамический фильтр
Сетевой уровень	Фильтрация пакетов	Экранирующий маршрутизатор, пакетный фильтр
Канальный уровень	Сегментация трафика	Управляемый (экранирующий) коммутатор

Фильтры пакетов сетевого уровня и маршрутизаторы позволяют выполнять функцию фильтрации по IP-адресу, портам, типу протокола и т.д. Недостатками пакетных фильтров являются ограниченная функциональность сетевого и транспортного уровней и уязвимость к атакам подмены IP-адреса.

Пакетные фильтры сеансового уровня позволяют выполнять фильтрацию с учетом большого числа параметров фильтрации (соответствующих сеансу).

Посредники – промежуточные сетевые средства, которые устанавливают собственное соединение и обрабатывают трафик на дополнительном устройстве. Это, в свою очередь, позволяет выполнять следующие задачи:

- аутентификацию;
- асинхронную, взаимодействие клиентов и серверов;
- трансляцию (и скрытие) адресов;
- переадресацию с целью перераспределения нагрузки на сеть;
- хеширование с целью повышения производительности обмена;
- регистрацию трафика.

В то же время использование посредников требует решения задачи обеспечения требуемой производительности по периметру сети, так как трафик вторично обрабатывается на дополнительном устройстве.

Особое внимание стоит уделить технологии маршрутизации, реализуемой посредником. В соответствии с ним выполняется трансляция сетевых адресов (Network Address Translation, NAT), т.е. внутренний адрес хоста заменяется личным адресом посредника. Другими словами, NAT реализует политику скрытия от внешней сети внутренних сетевых адресов и позволяет назначать посреднику один IP-адрес для внутренней сети. Трансляция адресов может быть назначена статически и динамически.

К посредникам сеансового уровня можно отнести посредника, SOCKet Secure (SOCKS5), который имеет высокую производительность, эффективное оборудование, скрывающее адреса, и возможность выделения TCP/UDP-трафика. Посредники HTTP / HTTPS и посредники FTP широко распространены в качестве прикладного посредника. Эти посредники позволяют фильтровать по контенту прикладного протокола.

Инспекторы состояния (фильтры с расширенными возможностями сеансового уровня) выполняют интеллектуальную фильтрацию на основе данных из заголовков протокола сеансового уровня. Это позволяет получить эффект фильтрации на вышестоящих уровнях. Такие межсетевые экраны не требуют установки посредника. Таким образом, производительность сети не снижается, но необходимый уровень безопасности обеспечивается. Удобство масштабирования также можно добавить к преимуществу инспекторов состояния.

В практике обеспечения межсетевой защиты информационных ресурсов можно встретить понятие UTM – устройства (Unifield Threat Management) и межсетевого экрана следующего поколения (Next Generation, NG firewall).

UTM – комплексное решение проблемы защиты периметра устройства. Помимо модулей межсетевого экранирования, в его состав могут входить системы обнаружения вторжений, потоковый антивирус, решения для защиты от спама, криптошлюз и т.д.

NG firewall схож с UTM и предназначен для объединения техники фильтрации портов, систем предупреждения вторжений и фильтрации трафика на уровне приложений.

Виртуальные частные сети. Под виртуальной частной сетью (Virtual Private Network, VPN) понимается средство защиты передаваемых данных путем создания временного защищенного канала связи на базе механизмов инкапсуляции данных, а также

дополнительной аутентификации, шифрования, контроля целостности. Как следует из названия, основная идея VPN состоит в том, чтобы временно (во время сеанса) инкапсулировать передачу данных, то есть создать защищенный туннель путем объединения сетевого пакета одного уровня в один пакет более высокого уровня.

Именно возможность организации временного туннеля демонстрирует преимущество перед организацией постоянного защищенного канала или аренды, выделенной линии, а инкапсуляция пакета данных в пакет вышестоящего уровня позволяет легко реализовать требования по шифрованию и контролю целостности передаваемых данных.

Принята классификация виртуальных частных сетей, в основном, по уровням модели OSI и способом подключения. По подключению различают способы «точка-точка» («узел-узел»), «точка-сеть» и «сеть-точка». В табл. 5.2 представлены наиболее популярные протоколы виртуальной частной сети.

PPTP (Point-to-Point Tunneling Protocol) – протокол туннелирования канального уровня типа «точка-точка». Этот протокол инкапсулирует кадры PPP в IP-пакеты, используя дополнительное TCP-соединение для обслуживания туннеля. Поддерживает различные протоколы удаленного доступа для аутентификации клиентов, включая протокол MSCHAPv2. При шифровании поддерживается протокол MPPE, реализующий алгоритм RC4.

Таблица 5.2

Протоколы виртуальной частной сети

Уровень модели OSI	**Базовый протокол туннелирования**	**Средства шифрования**
Сеансовый уровень	SOCKS	Использует нижележащие протоколы
Транспортный уровень	SSH	AES, 3DES, Blowfish
	SSL/TLS	AES, 3DES, IDEA, RC4 и др.
Сетевой уровень	IPSec (ESP)	AES, 3DES и др.
Канальный уровень	L2TP	Использует вышестоящие протоколы
	PPTP	MPPE (RC4)

L2TP (Layer 2 Tunneling Protocol) – протокол туннелирования канального уровня, который инкапсулирует кадры PPP в пакеты

сетевого уровня. К достоинству протокола относят поддержку приоритетов доступа и мультипротокольность (теоретически независимость от IP). Механизм шифрования делегируется вышестоящему уровню, что может быть реализовано, например, с использованием аппарата IPSec. В отличие от PPTP, в сетях TCP / IP этот протокол ориентирован к транспортному протоколу UDP.

Протокол IPSec (IP Security) работает в двух режимах – транспортном и туннельном. В транспортном режиме (этот режим используется для установления соединений между хостами) IPSec может использоваться для защиты туннелей типа «точка-точка», организованных каким-нибудь другим способом, в частности, L2TP, который не имеет функции шифрования. Туннельный режим позволяет создавать соответсвенные туннели, в которых весь зашифрованный пакет инкапсулируется на уровень выше для доставки адресату.

Дополнительные средства, обеспечивающие безопасность сети. *Система обнаружения вторжений (Intrusion Detection System, IDS).* В основе IDS лежит база данных атак, содержащая соответствующие шаблоны, сигнатуры или профили, и именно с этой базой данных сравниваются данные, полученные от сенсоров. Следовательно, эффективность IDS зависит от репутации базы данных атак. Для обнаружения вторжений можно использовать следующие методы:

- сигнатурный метод – обнаружение вторжений по набору данных, характерных для какой-либо атаки;
- метод выявления аномалий – выявление, не характерных для нормального состояния признаков;
- метод на основе политик безопасности – выявление нарушений параметров, определенных в политике безопасности.

По уровню мониторинга IDS-системы делятся на:

- IDS сетевого уровня (Network based IDS, NIDS);
- IDS, уровня узла (Host based IDS, HIDS).

NIDS может защищать хосты через мониторинг сетевого трафика, поступающего из нескольких хостов, подключенных к сегменту сети. HIDS работает с информацией, собранной с единственного компьютера, в основном из журналов операционных систем и системы защиты информации, профиля пользователя и т.д. Поэтому, если использование NIDS считается удобным при

определении компьютерных атак, то HIDS используется для фиксации достоверных фактов несанкционированного доступа.

IDS активного (in-line) типа называют системой предупреждения вторжений (Intrusion Prevention System, IPS).

Средства анализа защищенности. Использование различных средств анализа защищенности для выявления потенциальных и реальных уязвимостей по техническому аудиту специалистов. Существуют следующие классы средств анализа защищенности:

- сетевые сканеры уязвимостей;
- сканеры безопасности веб-приложений;
- средства анализа конфигурации системы;
- специальные средства тестирования.

Сетевые сканеры уязвимостей – специальные программные средства, в которых участвуют в качестве входной информации список сканируемых IP-адресов, а в качестве выходной информации отчет об обнаруженных уязвимостях. Основной принцип работы – определение точной версии программного обеспечения, установленного на удаленном узле, и поиск информации об уязвимостях, характерных для этой версии программного обеспечения, в обновляемой локальной базе уязвимостей.

Сканеры безопасности веб-приложений – специальные программные средства, которые анализируют структуру веб-систем. В результате выявляются потенциальные варианты ввода информации, и формируется запрос на использование уязвимости.

Средства анализа конфигурации системы – программа, оценивающая безопасность системы путем ее настройки. Такое решение может быть представлено в виде комплексного продукта или локального скрипта (сценария).

Специальные средства тестирования:

- программы online и o offline подбора паролей;
- фреймворки использования уязвимостей;
- программы, осуществляющие определенные сетевые атаки (например, ARP-spoofing);
- локальный HTTP-прокси и т.д., для изменения HTTP-запросов, отправляемых на веб-сервер.

Существуют различные онлайн-базы уязвимостей. База данных уязвимостей CVE (Common Vulnerabilities and Exposures, cve.mitre.org) пользуется популярностью.

Системы предотвращения утечки информации (Data Leakage Prevention, DLP). Эти системы используются для выявления и блокировки коммерческой, профессиональной или другой секретной информации, которые незаконно отправляются во внешнюю сеть. DLP система по схеме подключения похожа на IDS решения – анализирующая информация может собираться на сетевом уровне или на уровне хоста.

Для контроля потоков информации, чтобы определить наличие в них конфиденциальной информации, используются два метода:

- обнаружение по меткам, приведенным в документе;
- обнаружение по контенту набора данных.

Согласно первому методу, информация изначально разбивается на категории и маркируется. В этом случае к конфиденциальному документу (например, файлу, записи базы данных и т.д.) предварительно ставится соответствие какой-либо неотчуждаемый формальный признак (например, контрольная сумма, инвентарный номер, гриф конфиденциальности). Затем при обнаружении данного признака в передаваемом информационном потоке соответствующий документ блокируется. Такой подход способен защитить документ только в целом. Достоинством подхода является снижение юридических рисков и невысокий уровень ложных срабатываний различного рода.

Ложные цели или ловушки (honeypot). Используются для провоцирования атак со стороны злоумышленников с целью их выявления, а также методов взлома.

При классификации ложных целей их интерактивность используется как признак, то есть выделяются следующие ловушки:

- интерактивные ловушки;
- ловушки с низким уровнем интерактивности;
- ловушки с высоким уровнем интерактивности.

Ловушки с низким уровнем интерактивности могут быть эмуляцией одной сетевой службы, например, сервиса FTP. Хотя простота размещения и контроля является преимуществом таких ловушек, их недостатком является то, что они часто могут использоваться только для обнаружения факта атаки.

Ловушки с высоким уровнем интерактивности можно рассматривать как виртуальную машину с полноценной операционной системой и набором сервисов. Такие ловушки

позволяют собрать много информации о намерениях злоумышленника (особенно, если с ним установлена интеллектуальная обратная связь).

«Пустые» сети (DarkNet) являются отдельным классом ловушек. В соответствии с ними, в корпоративной сети выделяется диапазон внешних адресов, которые фактически не используются при решении бизнес-задач. Любое обращение к «Пустым» сетям означает ошибку конфигурации или незаконную деятельность.

Следует отметить, что IDS и DLP решения рассчитаны на известный класс атак. На практике возникает вопрос сбора любых событий безопасности и надежности функционирования информационной системы. К таким системам относятся:

- системы управления журналами (log management). Эти системы предназначены для организации централизованного сбора событий информационной безопасности;
- системы управления информацией о безопасности (Security Information Management, SIM). Эти системы предназначены для централизованного сбора событий информационной безопасности, а также для формирования и анализа различных отчетов;
- системы управления информацией о безопасности и о событиях безопасности (Security Event Manager, SEM). Эти системы предназначены для мониторинга в режиме реального времени, корреляции событий информационной безопасности;
- системы управления информацией безопасности и событиях безопасности (Security Information and Event Management, SIEM). Эти системы являются следующим шагом в развитии систем мониторинга, поскольку они комбинируют функционал SEM и SIM.

Можно добавить, что определяющим механизмом для межсетевых экранов является фильтрация, для VPN – инкапсуляция, а для SIEM – корреляция.

5.4. Безопасность беспроводной сети

Типы беспроводных сетей. Известно, что вскоре после изобретения радио стало возможным осуществлять телеграфную связь без проводов. Фактически тот же принцип используется для передачи текущего цифрового кода по радиоканалу, но пропускная способность передачи данных увеличилась в несколько раз.

По радиусу действия и назначению современные беспроводные сети можно разделить на:

- персональные (Wireless Personal Area Network, WPAN);
- локальные (Wireless Local Area Network, WLAN);
- городские (Wireless Metropolitan Area Network, WMAN);
- глобальные (Wireless Wide Area Network, WWAN) (рис. 5.6).

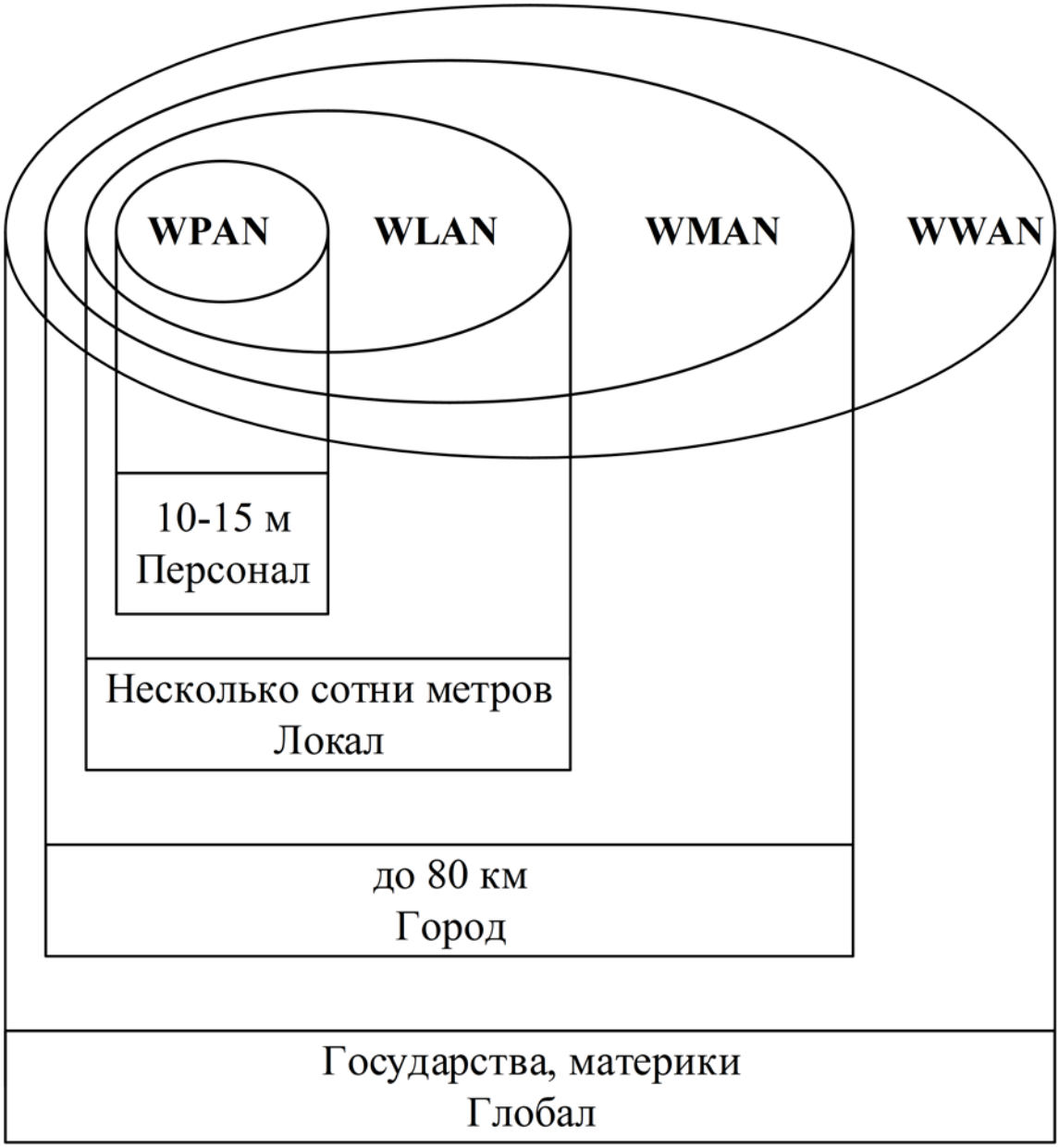


Рис.5.6. **Классификация беспроводных сетей**

В табл. 5.3 приведены характеристики указанных выше беспроводных сетей.

Таблица 5.3

Основные характеристики беспроводных сетей

Беспроводные сети / Характеристики	**WPAN (персональные беспроводные сети)**	**WLAN (локальные беспроводные сети)**	**WMAN (городские беспроводные сети)**	**WWAN (глобальные беспроводные сети)**
Область применения	Замена проводки периферийных устройств	Мобильные расширения проводных сетей	Широкополосный беспроводной доступ	Мобильный доступ в Интернет за пределами здания
Технологии	Bluetooth, UMB, ZigBee	Wi-Fi (802.11)	WiMax (802.16), MBWA-m (802.20)	GSM, GPRS, WCDMA, EDGE, HSPA +, WiMax, LTE

Основные угрозы безопасности информации в мобильных сетях. Хотя для создания безопасного беспроводного приложения требуется выявление всех потенциальных направлений беспроводной «атаки», приложения никогда не будут полностью безопасны. Тем не менее, тщательное изучение угроз в беспроводных технологиях, помогает повысить уровень защиты в каждом случае. Следовательно, проанализировав потенциальные угрозы, необходимо построить сеть таким образом, чтобы быть готовым предотвратить атаки, и защитить от нестандартных «атак».

Неконтролируемая территория. Основное различие между проводными и беспроводными сетями – наличие абсолютно неконтролируемой территории между крайними точками беспроводной сети. В достаточно большом пространстве сотовых сетей беспроводная среда никогда не контролируется. Современные беспроводные технологии предлагают ограниченный набор средств управления сетевого пространства. Это позволяет атакующим, находящимся вблизи беспроводных структур, осуществить атаки, не возможные в проводном мире.

Несанкционированное вторжение. Если защита беспроводной сети не реализована, то любое устройство с беспроводным подключением может использовать ее. В этом случае, как правило,

закрытый вещательный диапазон входа может составлять до 50-100 метров, во внешней зоне – до 300 метров.

Скрытое подслушивание. Наиболее распространенной проблемой в открытой и неуправляемой среде, такой как беспроводные сети, является наличие анонимных атак. Чтобы перехватить передачу злоумышленник должен находиться рядом с передатчиком. Перехваты такого типа невозможно зарегистрировать, и предотвратить их еще труднее. Использование антенн и усилителей позволяет злоумышленнику в процессе перехвата находиться на большом расстоянии от цели.

Так как не все протоколы, используемые в беспроводных сетях, являются безопасными, метод скрытого подслушивания может быть очень эффективным. Например, если беспроводная локальная сеть, использует протокол WEP, существует большая вероятность того, что сеть будет подслушиваться.

Принуждение к отказу от обслуживания. Во всей сети, включая базовые станции и клиентские терминалы, возникает такая сильная интерференция, что станции не могут связываться друг с другом. Атака типа DoS может полностью отключить сеть. Эта атака отключает все коммуникации в определенном районе (рис.5.7).

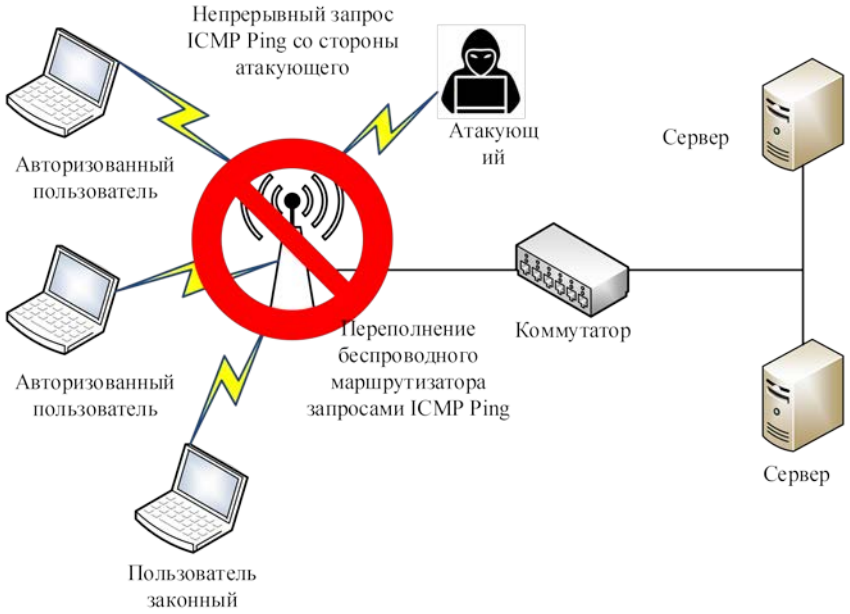


Рис.5.7. **Осуществление DoS-атаки на беспроводную сеть**

Атака посредника. Атаки MITM похожи на атаки вторжения, описанные выше, они могут принимать множество различных форм и используются для нарушения конфиденциальности и целостности

сеанса связи. Атаки MITM намного сложнее, потому что для их выполнения требуется подробная информация о сети. Злоумышленник обычно выполняет идентификацию одного из сетевых ресурсов. Когда жертва атаки начинает соединение, мошенник перехватывает его и завершает соединение с желаемым ресурсом, а затем пропускает все соединения с этим ресурсом через свою собственную станцию (рис. 5.8). При этом атакующий может отправить информацию, изменить то, что было отправлено, или подслушать все разговоры, а затем расшифровать их.

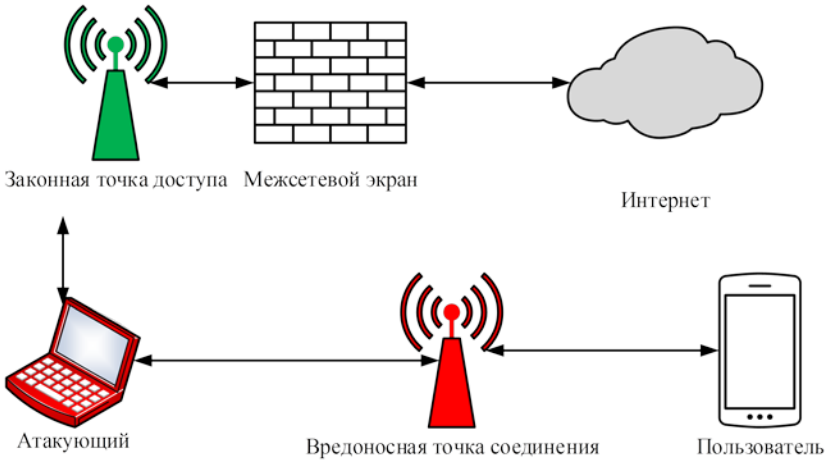


Рис.5.8. **Осуществление атаки MITM**

Ложные точки доступа в сеть (вредоносная двойная атака). Опытный атакующий может организовать ложную точку доступа, имитируя сетевые ресурсы. Абоненты, без сомнения, обратятся к этой ложной точке доступа и сообщат ей важные реквизиты, например, данные аутентификации. Этот вид атаки иногда осуществляется в сочетании с прямым глушением с целью «удушения» истинной точки доступа сети (рис. 5.9).

Проблемы с роуминга. Еще одно важное различие между беспроводной сетью и проводной сетью – способность пользователя перемещаться, не отключаясь от сети. Концепция роуминга практически одинакова в различных стандартах беспроводной связи CDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications) и беспроводном Ethernet. Многие сетевые приложения TCP/IP требуют, чтобы IP-адреса сервера и клиента не менялись. Однако в процессе роуминга в сети абонент обязательно уйдет из одного места и перейдет в другое.

Использование мобильных IP-адресов и других механизмов роуминга в беспроводных сетях основано на этом требовании.

Рис.5.9. **Вредоносная двойная атака**

Взгляд через плечо. При подключении к беспроводной сети в общественных местах нарушитель может легко получить настройки подключения (посмотрев через плечо). Это позволяет полноценно использовать беспроводную сеть.

Меры предотвращения проблем безопасности, при использовании беспроводных сетей *Изменение пароля текущей настройки.* У большинства сетевых устройств, в том числе беспроводных сетевых устройств, есть текущий пароль настройки, и они известны всем. Иногда администратор сети забывает изменить эти пароли, и в результате возникает серьезная проблема. Поэтому перед использованием сетевых устройств необходимо изменить текущий установленный пароль.

Ограничение доступа. Важно обеспечить то, чтобы использование сети было разрешено только тем, у кого есть доступ. Каждое устройство имеет встроенный адрес MAC (Media Access Control), доступ к которому можно получить, проверив эти адреса. Другими словами, память беспроводного сетевого устройства будет содержать MAC-адреса устройств, которые могут быть

подключены. Те, у кого новый адрес, не смогут подключиться к этой сетевой точке.

Шифрование данных, передаваемых по сети. Если все данные, передаваемые по беспроводной сети, будут зашифрованы, можно будет защитить их от несанкционированного чтения. В беспроводных локальных сетях данные между точкой сети и пользовательскими устройствами обычно передаются в зашифрованном виде на основе протоколов Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 и WPA3. Несмотря на то, что WPA3 считается надежным, остальные протоколы, которые на практике считаются слабыми, также широко применяются.

Защита беспроводного сетевого устройства (SSID, Service Set Identifier). Для предотвращения легкой управляемости беспроводной сети за пределом сети, требуется неразглашение SSID. Все Wi-Fi устройства имеют возможность для защиты SSID, это затрудняет атакующему найти беспроводную сеть. Эту величину не рекомендуется оставлять в текущем состоянии и в меньшей мере требуется обновить SSID.

Установка средства межсетевого экрана. В беспроводных устройствах рекомендуется установка межсетевого экрана, основанного непосредственно на хосте или модеме для домашней сети. Эта защитная мера предотвращает прямое соединение атакующего к сети.

Осторожная реализация обмена файлом. В случае отсутствия необходимости обмена файлом, данная возможность должна быть отключенной. Обмен файлом всегда необходимо реализовать из персональной или домашней сети. Обмен файлом в открытой сети не рекомендуется. Кроме того, необходимо обеспечить защищенность каждого передаваемого файла на основе пароля (блокировки файла).

Регулярное обновление программного обеспечения, используемого в точке беспроводной сети. Производители постоянно разрабатывают новые версии для устройств, и они предназначены для предотвращения проблем безопасности в существующей версии. По этой причине рекомендуется на программной основе обновлять устройства беспроводной сети.

Прислушиваться к рекомендациям Интернет-провайдера или производителя беспроводного сетевого устройства. Обычно

производители беспроводных сетевых устройств предоставляют рекомендации по безопасному использованию устройств на своих веб-сайтах. Следование этим рекомендациям в большинстве случаев поможет предотвратить потенциальную проблему безопасности.

5.5. Риски и управление рисками

Риск – одно из понятий, связанных с кибербезопасностью. Ниже приводится подробное описание понятия риска и управления им.

Риск – ожидание того, что при определенных условиях угроза нанесет потенциальный ущерб ресурсам. Кроме того, риск можно понимать следующим образом:

- *Риск* – событие, которое может привести к возникновению, потере или другим неблагоприятным последствиям угрозы или события в результате внутренних или внешних обязательств.
- *Риск* – вероятность угрозы внутренней или внешней уязвимости, повреждающей источник.
- *Риск* – вероятность события и влияние этого события на активы информационных технологий.

Между понятиями риска, угрозы, уязвимости и воздействия существует взаимосвязь, которую можно выразить следующим образом:

$$\text{РИСК} = \text{Угроза} \times \text{Уязвимость} \times \text{Воздействия}.$$

С другой стороны, влияние события на актив информационных технологий является результатом уязвимости актива или для заинтересованной стороны стоимости актива, то есть:

$$\text{РИСК} = \text{Угроза} \times \text{Уязвимость} \times \text{Стоимость актива}.$$

Риск объединяет следующие два фактора:

- вероятность возникновения вредоносного события;
- и вероятность последствий вредоносного события.

Воздействие риска. Риск влияет на процесс нормальной реализации и стоимость проекта или ожидаемую стоимость. Воздействие риска возникает из-за среды, которая наносит вред организации, процессу или системе. Воздействие указывает на серьезность вероятности того, что риск будет обнаружен.

Частота риска. Классификация рисков с точки зрения выявления и оценки рисков основана на их частоте и количестве

повторений. Частота и множественность являются важными особенностями мониторинга рисков, и риски делятся на две группы: *минорные риски* – те, которые не требуют внимания, и *мажорные риски* – те, которые требуют особого внимания и мониторинга.

Уровень риска. Уровень риска – оценка результирующего воздействия на сеть (или систему), выраженная следующим уравнением:

$$\text{Уровень риска} = \text{результат} \times \text{вероятность}.$$

Существует 4 уровня риска: экстремально высокий, высокий, средний и низкий.

Экстремально высокий или *высокий* риск требует специальных целенаправленных контрмер для сведения к минимуму возникновение и неблагоприятное последствие. Риски на этом уровне имеют высокую вероятность сильного или умеренного воздействия. Риски на этом уровне представляют собой серьезный риск и, следовательно, должны быть немедленно выявлены и приняты контрмеры.

Риски среднего уровня могут быть событием низкого результата с высокой вероятностью или событием высокого результата с низкой вероятностью. При отдельном рассмотрении низко результатные события с высокой вероятностью мало влияют на стоимость проекта или ожидаемый результат. События высокого результата с низкой вероятностью требуют постоянного мониторинга. Хотя риски среднего уровня не требуют немедленных действий, защиту требуется установить на ранней стадии.

Риски низкого уровня – категория рисков, на которую обычно можно не обращать внимания, или обращать внимание при последующих оценках, и их устранение не требует краткосрочного осуществления или чрезмерных затрат.

Матрица риска определяет вероятность возникновения рисков в зависимости от их результатов и воздействия, а также графически представляет серьезность риска и уровень защиты от него. Матрица рисков – простой процесс, используемый для увеличения вероятности возникновения риска, помогающий принимать контрмеры. Матрица рисков позволяет выявлять риски на разных уровнях и группировать по степени серьезности (табл. 5.4).

Представленная матрица рисков позволяет наглядно представить и сравнить риски, и каждая ячейка в ней состоит из комбинации вероятностей и величин последствий. Серьезность риска зависит от его вероятности и уровня воздействия. Они разделены на 5 групп по вероятности появления в матрице рисков. Соответственно, риск исхода также делится на 5 уровней.

Таблица 5.4

Матрица рисков

Вероятность (ясность)		**Последствия / влияние**					
			Не важно	Низкий	Средний	Высокий	Серьезный
81–100%	**Вероятность (неясность)**	Очень высокий	Низкий	Средний	Высокий	Очень высокий	Очень высокий
61–80%		Высокий	Низкий	Средний	Высокий	Высокий	Очень высокий
41-60%		Равный	Низкий	Средний	Средний	Высокий	Высокий
21-40%		Низкий	Низкий	Низкий	Средний	Средний	Высокий
1-20%		Очень низкий	Низкий	Низкий	Средний	Средний	Высокий

Управление рисками. Управление рисками – процесс выявления, оценки, реагирования на риски и побуждения организации реагировать на потенциальные воздействия. Управление рисками занимает важное место в жизненном цикле безопасности, это постоянный и даже сложный процесс. Хотя риски различаются от организации к организации, обучение управлению рисками является общим для всех организаций. Основными задачами управления рисками являются:

- выявление потенциальных рисков;
- определение воздействия риска и помощь организациям разрабатывать более эффективные стратегии и планы управления рисками;
- использование методов, средств и технологий управления рисками для классификации рисков и оказания им помощи в зависимости от степени серьезности;
- понимание, анализ рисков и регистрация выявленных рисковых событий;
- контроль рисков и борьба против воздействия рисков;

- разработка стратегии, предупреждения сотрудников службы безопасности и управления рисками.

Управление рисками предусматривает системный подход к их выявлению и имеет следующие преимущества:

- фокусируется на области потенциального воздействия риска;
- переадресовывает риски по уровням;
- улучшает процесс выявления рисков;
- помогает сотруднику службы безопасности эффективно действовать при возникновении непредвиденных обстоятельств;
- позволяет эффективно использовать ресурсы.

Важные роли и обязанности в управлении рисками. Роли и обязанности в управлении рисками распределяются между исполнителями следующим образом:

Главный управляющий. Главный управляющий является руководителем процесса управления рисками в организации и разрабатывает политику и методы, необходимые для выявления рисков до их возникновения. Кроме того, в его задачу также входит проведение необходимых мер для сдерживания потенциальных рисков в будущем.

Директор по информационным технологиям. Обладатель этой должности несет ответственность за реализацию политики и планов, необходимых для поддержки информационных и компьютерных технологий организации. Основная ответственность этого должностного лица заключается в обучении сотрудников технике безопасности и управлении воздействием потенциальных рисков на бизнес-процессы, связанные с информационными технологиями.

Владельцы систем и информации. Обязанности владельцев систем и информации заключаются в основном в мониторинге планов и политик, разработанных для информационных систем, и включают следующие обязанности:

- участие во всех переговорах, связанных с процессом управления настройкой;
- хранение учета компонентов информационных технологий;
- изучение всех изменений в информационных системах и их воздействий;
- подготовка отчетов о состоянии безопасности для всех систем;

- обновление мер безопасности, необходимых для защиты информационных систем;
- регулярное обновление документации по безопасности;
- проверка и оценка для обеспечения эффективности существующих мер безопасности.

Бизнес и функциональные менеджеры. Обладатели этой должности несут ответственность за поддержку всех процессов управления в организации и получают поддержку от руководства организации в выполнении этой задачи. Типы функционального менеджера:
- менеджер группы развития;
- менеджер по продажам;
- менеджер по обслуживанию клиентов.

Менеджеры программы безопасности ИТ и директор отдела компьютерной безопасности. Обладатели этой должности поддерживают владельцев информационных систем, выбирая меры безопасности для защиты системы.

Практиканты безопасности ИТ. Специалисты по безопасности ИТ осуществляют личную, физическую и информационную безопасность в организации и несут ответственность за:
- создание более эффективных методов безопасности в организации;
- разработку методов, полностью соответствующих стандартам организации;
- проверку подходов организации к безопасности для управления рисками и бизнес-планированию;
- захват и запись инцидентов безопасности;
- определение ролей и ответственности за безопасность в организации;
- контроль всех мер безопасности в организации.

Наставник по безопасности. Наставник по безопасности проводит тренинги и образовательные курсы в организации. Рекомендуется, чтобы эту задачу выполняли, как правило, специалисты данной области.

Важные показатели риска. Важные показатели риска являются основными детерминантами в процессе эффективного управления рисками, указывающими на степень риска движений на начальных этапах. Правильное выявление важных показателей

риска требует понимания цели организации. Это помогает в организации реализовать в качестве меры вероятности риска следующее:

- определить влияние инцидента;
- предупреждать о предельном значении;
- пересмотр рисковых событий.

Важный показатель риска должен быть рассчитан точно и отражать негативное влияние на показатели эффективности организации. В этом случае показатель деятельности организации является показателем оценки процесса, посредством которого организация достигает своих целей.

Этапы управления рисками. Управление рисками – непрерывный процесс, который требует успешной реализации на каждом этапе. Он позволяет избежать риска на приемлемом уровне за счет использования идентифицированной и активно работающей программы безопасности. Процесс управления рисками делится на следующие основные четыре этапа:

1. Выявление рисков.
2. Оценка рисков.
3. Предотвращение рисков.
4. Мониторинг и пересмотр рисков.

Каждая организация проходит указанные выше этапы в процессе управления рисками.

Выявление рисков. Первым шагом в управлении рисками является выявление риска до того, как он нанесет вред организации. Поскольку процесс выявления рисков зависит от способностей ответственных специалистов, он отличается в разных организациях по-разному. Выявление риска включает в себя источник, причины, результат и т.д. внутренних и внешних рисков, которые влияют на безопасность организации. Риски обычно возникают в следующих 4 важных областях:

- *среда* – риски, связанные со средой, сочетают в себе недостатки на рабочем месте, различные нарушения, горячую/ холодную среду, дым, низкое освещение и опасность электричества и т.д.;

- *оборудование* – к рискам, связанным с оборудованием можно отнести низкие эксплуатационные расходы, неисправность оборудования, его недоступность и несоразмерность функций;

- *клиент* – риски, связанные с клиентами, обычно возникают в результате значительных изменений, неожиданных действий и слабого взаимодействия;

- *задачи* – примеры рисков, связанных с задачами, включают риски, связанные с недостаточным временем выполнения, повторяющимися задачами, планированием работы и недостаточным количеством сотрудников.

Выявление рисков уменьшает различные отклонения в процессе управления рисками, что, в свою очередь, снижает вероятность будущих влияющих факторов. Существует множество способов выявления рисков, на основе которых были разработаны различные программные средства. Большинство процессов выявления рисков осуществляется специально сформированной командой. Процесс выявления рисков основан на ряде факторов, таких как состояние сети и способность членов команды управлять рисками.

Оценка рисков. На этапе оценки рисков оцениваются риски в организации, и рассматривается влияние или вероятность возникновения этих рисков. Оценка рисков – непрерывный продолжающийся процесс, который определяет привилегии реализации планов управления рисками. Оценка рисков определяет их количественную и качественную ценность. Каждая организация должна принять свой собственный процесс оценки рисков для выявления, классификации и устранения рисков.

Оценка риска определяет тип представленного риска, вероятность и размер риска, его уровень и план контроля. Организации обычно выполняют процесс оценки риска, когда риск идентифицирован и не может быть немедленно отслежен. Все средства массовой информации необходимо будет обновить в течение определенного периода времени после оценки рисков.

После оценки рисков они классифицируются в соответствии с количественным ущербом, который они нанесут организации. Классификация помогает бороться с рисками и распределять ресурсы. Уровень представленных рисков будет зависеть от их количества:

- если невозможно сразу устранить или исключить риски 1-2 уровня, необходимо снизить уровень его опасности за счет контролирующих воздействий;

- необходимо устранить риски 3-4 уровня или взять риск под контроль на некоторое время;
- риски уровня 5-6 следует устранять, когда это возможно, или, если это невозможно, риск следует контролировать.

Оценка рисков осуществляется в следующие два этапа:

Анализ риска: этап определения характера риска и расчета степени его возникновения, помогает контролировать риски.

Классификация рисков: этап анализа рисков в процессе определения их количественного рейтинга и проектирование мер противодействия.

Предотвращение рисков. Процесс предотвращения рисков является первым обращением к тем, кто обладает высоким количественным уровнем, обеспечивающим отбор и осуществление соответствующего контроля с целью модификации выявленных рисков. Принятие решения на этом этапе основывается на результатах оценки риска. Основной задачей данного этапа является выявление контрмер для контроля серьезно рассматриваемых рисков, а затем, для индивидуального устранения, мониторинга и пересмотра рисков, осуществляется их разделение на уровни. Перед устранением рисков необходимо следующее:

- выбор соответствующего метода защиты;
- назначение ответственного за способ защиты;
- учет стоимости защиты;
- обоснование достоинства метода защиты;
- определение вероятности достижения успеха;
- определение метода измерения и метода оценки.

Если требуется устранить выявленные риски, необходимо будет постоянно пересматривать и разрабатывать план управления рисками. Различные методы защиты предлагают такие возможности, как избежание рисков, их минимизация и перекладывание ответственности другому лицу.

Для того чтобы снизить или минимизировать риски со стороны сотрудников требуется:

- разработка плана контроля рисками;
- определение влияния рисков на предоставляемые услуги;
- установка строгих ограничений на выполнение плана контроля рисками;
- осуществление стратегии контроля рисками;

- выявление поведения клиентов при контроле рисками;
- установление связи с поддерживающим персоналом во время контроля рисков;
- полное документирование части процесса контроля рисками.

Мониторинг и пересмотр рисков. Эффективный план управления рисками требует мониторинга и пересмотра рисков при гарантированном выполнении выявлении и оценки рисков. Мониторинг рисков предоставляет следующие возможности:

- определяет возможность возникновения новых рисков;
- гарантирует реализацию соответствующего метода предотвращения рисков;
- вероятность, влияние, статус и раскрытие риска.

Посредством пересмотра рисков гарантируется:

- оценка эффективности стратегий управления рисками;
- управление осведомленностью о высоко вероятных рисках.

Фреймворк (структура) управления рисками в организации *(Enterprise Risk Management Framework, ERM Framework).* Фреймворк управления рисками определяет меры по реализации, специфичные для подхода организации к управлению рисками, и обеспечивает структурный процесс, который объединяет деятельность по информационной безопасности и управлению рисками в организации. Фреймворк управления рисками в организации выявляет, анализирует и реализует следующие действия:

- избежание рисков путем отмены рискованных действий;
- снижение риска за счет минимизации воздействия или вероятности риска;
- предоставление стандартов процесса управления рисками.

Основными целями структуры управления рисками в организации являются:

- объединение управления рисками в организации с управлением деятельностью организации;
- связывание преимуществ управления рисками;
- определение ролей и ответственности в организации за управление рисками;
- стандартизация отчетности о рисках и процесса развития;
- установка стандартных подходов к управлению рисками в организации;

- оказание содействия ресурсам в управлении рисками;
- установка области применения и приложений управления рисками в организации;
- правоведение периодических проверок для улучшения управления рисками в организации.

На практике в организации широко используются в качестве фреймворков управления рисками NIST ERM, COSO ERM и COBIT ERM.

Информационные системы управления рисками (Risk Management Information Systems, RMIS). RMIS – информационная система управления, которая предоставляет возможность управления информацией, анализ и получение информации о риске для сети организации. Организации для оптимизации риска, объединяют RMIS с фреймворком управления рисками. Системы RMIS имеют следующие преимущества:

- повышает надежность данных за счет уменьшения избыточности данных и ошибок;
- снижает затраты в организации за счет улучшенного управления сообщениями через RMIS;
- RMIS помогает в эффективном использовании политик управления рисками в соответствии со стандартами организации.

RMIS формирует отчеты по различным факторам, и эти отчеты позволяют организации иметь целостное представление о сетевых рисках и управлять ими. Типы сгенерированного отчета RMIS будут зависеть от типа отправленного ему запроса. RMIS формирует следующие типы отчетов:

- *Стандартные отчеты:* формирует стандартные отчеты в ответ на отправленные общие запросы. Этот отчет не состоит из сгруппированных данных;
- *Специальные отчеты:* формирует специальные ответы на специальные запросы, содержащие информацию, принадлежащую разным группам

На практике широко используются различные формы системных инструментов RMIS. В качестве примера, можно привести средства Aon Enterprise Risk Management, Stars RMIS, RiskEnvision, RiskonnectRMIS, INFORM, Traveler’s e-CARMA.

Контрольные вопросы

1. Компьютерная сеть и ее типы.
2. Топология сети и ее типы.
3. Сетевые устройства и их основные функции.
4. Основные сетевые протоколы и их функции.
5. Объясните понятия угрозы, уязвимости и атаки.
6. Основные причины возникновения сетевых проблем.
7. Типы угроз и приведите их примеры.
8. Как нарушение сетевой безопасности влияет на деятельность бизнеса?
9. Уязвимости сетевой безопасности и их типы.
10. Виды атак на безопасность сети.
11. Основная цель разведывательных атак.
12. Приведите примеры к атакам вторжения.
13. Какова основная цель атак с использованием вредоносных средств?
14. Основная задача межсетевого экрана.
15. Классификация межсетевых экранов.
16. VPN сеть и ее основные задачи.
17. Способы построения VPN сети.
18. Объясните понятие риска.
19. Объясните понятие уровня риска.
20. Объясните матрицу риска и ее основную задачу.
21. Управление риском и его основные этапы.
22. Фреймворк управления рисками в организации и ее основные задачи.
23. Приведите примеры информационных систем управления рисками.

ГЛАВА 6. МЕТОДЫ ОБЕСПЕЧЕНИЯ ДОСТУПНОСТИ

6.1. Понятие доступности и резервное копирование

Доступность. Компьютерная безопасность означает защиту информации и информационных систем от несанкционированного доступа, раскрытия, взлома, изменения или уничтожения, и ее наиболее важной целью является обеспечение конфиденциальности, целостности и доступности информации. Если компьютерные системы используются для хранения и обработки данных, то средства контроля безопасности используются для защиты от неправомерного использования данных. В свою очередь, важным является обеспечение доступности, которое позволяет информационным системам достигать своих целей.

Понятию доступность со стороны разных компаний и учеными дано различное определение, в частности:

- предоставить доступ тем, кому нужна конфиденциальная информация или ресурсы;
- своевременный и надежный доступ авторизованных пользователей к данным и информационным системам;
- не препятствовать доступу к системе уполномоченных лиц, имеющих законный доступ к объектам;
- гарантирование того, чтобы системы работали быстро и не были заблокированы для законных пользователей.

Хотя широкое внедрение информационных технологий во всех областях в настоящее время имеет важное значение для работы организации или предприятия, однако, если у организации имеются проблемы с информационными системами, ее деятельность может столкнуться со значительными убытками. Предположим, что хостинг-провайдеры обеспечивают 99% доступности в обслуживании услуги. Хотя это значение явно велико, оно означает 87 часов (3,62 дня) без обслуживания в год. За это время организация может по-разному понести ущерб, в зависимости от размера обслуживания. В приведенном выше случае, даже если достигается 99,9% доступности в обслуживании, наблюдается потеря 9 часов в год.

Снижение этих потерь в обслуживании важно не только для крупных корпораций, таких как Facebook или Amazon, но и для всех организаций. В частности, 30-минутный сбой Amazon.com в 2013 году обошелся компании в 2 миллиона долларов (66 240 $ за минуту).

Приведенные выше примеры показывают, насколько важно обеспечить доступность для любой организации. Высокая доступность сочетает в себе следующие 3 фактора:

- *отказоустойчивость:* этот фактор указывает на то, что система не выйдет из строя, даже если будет обнаружена ошибка;
- *гарантия предоставляемых услуг:* услуги, а также системы должны быть всегда доступны;
- *безопасность данных:* целостность данных в инфраструктуре, должна быть обеспечена даже в случае сбоя процессов и в работе сотрудников.

Доступность высокого уровня не допускает никакой ошибки. Другими словами, чтобы хостинг-провайдеры могли обеспечить доступность высокого уровня, они должны предотвратить сбой любого сетевого устройства (например, маршрутизатора или межсетевого экрана).

Атакой, нарушающей доступность системы или службы, является *атака принуждения к отказу в обслуживании (DoS),* основная цель которой заключается в отказе системе или сети предоставлять услуги законным пользователям. Эта атака реализуется на основе различных характеристиках системы и среды, с использованием разных методов и средств.

Рекомендуется принять комплексные меры защиты для предотвращения атаки принуждения к отказу в обслуживании и обеспечения доступности.

Резервное копирование. В настоящее время потеря данных является одной из основных проблем безопасности для организаций, в результате чего организация может понести огромные убытки. Поэтому со стороны организации требуется регулярное резервное копирование важных данных.

Резервное копирование данных – процесс копирования или хранения важных данных, позволяющий восстановить их в случае потери. Основная цель резервного копирования данных:

- вернуть систему в нормальное рабочее состояние после повреждения;

- восстановить важные данные, хранящиеся в системе, после их утери.

Хотя потеря данных в организациях характеризуется финансовыми последствиями и последствиями, связанными с клиентами, она может привести к потере личных файлов, фотографий и других ценных данных на персональном компьютере.

Потеря данных может быть вызвана следующими причинами:

- *человеческий фактор:* намеренное или случайное удаление данных, неправильное размещение носителей данных или неправильное управление базой данных;
- *злоумышленные действия:* модификация или кража важной информации в организации;
- *естественные причины:* отключение электроэнергии, случайное изменение программного обеспечения или повреждение устройства;
- *стихийные бедствия:* землетрясения, пожары и др.

Резервное копирование данных в организации или на персональном компьютере предоставляет следующие возможности:

- использовать важные данные даже в случае потери или повреждения;
- защита организаций от прекращения их деятельности и своевременное восстановление данных;
- восстановление потерянных данных в организации.

Идеальная стратегия резервного копирования данных включает в себя этапы от правильного выбора данных до гарантированного процесса восстановления данных. Хотя в разных организациях резервные копирования различаются, является важным обратить внимание на следующие особенности:

– стратегия резервного копирования данных должна обеспечивать возможность восстановления данных с любых внешних устройств. В качестве примера можно привести такие устройства как серверы, хост-машины, ноутбуки и т.д.;

– если данные потеряны в результате стихийного бедствия, стратегия резервного копирования не должна ограничиваться защитой от ограниченного числа инцидентов. Даже в случае стихийного бедствия стратегия должна включать методы восстановления данных;

– стратегия должна состоять из важных шагов по восстановлению данных на ранних этапах;

– низкая стоимость резервного копирования является финансовой поддержкой для организации;

– резервное копирование данных должно выполняться автоматически, чтобы быстро предотвратить потенциальную человеческую ошибку.

Выбор хранилища резервных копий в организациях является распространенной проблемой, и выбор неподходящего носителя резервных копий может привести к утечке данных. Выбор носителя для резервного копирования зависит от типа хранимых данных и основывается на следующих факторах:

- *стоимость:* каждая организация должна иметь средство резервного копирования, соответствующее ее бюджету. Наличие средств, размер которых превышает размер хранимых данных, приведет к непредвиденным затратам;

- *надежность:* организации должны убедиться, что их данные хранятся в средствах резервного копирования, которые работают без сбоя;

- *скорость:* организации должны выбирать средства хранения, которые требуют как можно меньшего вмешательства человека в процесс резервного копирования;

- *доступность:* при использовании инструмента резервного копирования после потери или повреждения данных могут возникнуть проблемы. Поэтому организациям следует обращать внимание на то, что средства резервного копирования всегда доступны для использования;

- *удобство:* организация должна выбрать удобное средство резервного копирования для использования. Это, в свою очередь, важно для обеспечения гибкости процесса резервного копирования.

В настоящее время для хранения резервных копий данных используются следующие средства:

Оптические диски (DVD, Blu-ray). DVD-диски могут хранить до 8,55 ГБ данных, и доступны только для чтения. Хотя преимущество этих устройств хранения данных основано на их низкой стоимости и простоте использования, их неспособность хранить большие объемы данных является их недостатком.

Портативные жесткие диски / USB-накопители. Портативные жесткие диски – хороший инструмент для хранения меньших объемов данных резервного копирования, чем диски DVD и Blu-ray. Флэш-диски бывают разных размеров и могут хранить большие объемы данных. Другой вариант использования жестких дисков – RAID (Redundant Array of Independent Disks).

Ленточные диски. Ленточные диски являются наиболее подходящими хранителями для резервного хранения данных и выполняют резервное копирование данных на уровне организации. Эти устройства хранения используются для хранения данных и приложений. Это хранилище резервных копий легко переносить, не требует участия пользователя в реализации и полностью автоматизировано. Его основным недостатком является его дороговизна для обычных пользователей и тот факт, что обычным компьютерам требуется дополнительное оборудование и программное обеспечение для его использования.

6.2. Технологии и методы резервного копирования данных

Большинство организаций осуществляют резервное копирование важных данных с помощью технологии RAID. Поскольку в технологии RAID данные хранятся в разных областях нескольких дисков, это упрощает операции IO (ввода-вывода). Технология RAID работает путем установки нескольких жестких дисков как одного логического диска. Эта технология позволяет хранить одни и те же данные сбалансированным образом по массиву дисков. Эта технология обычно предназначена для хранения данных на серверах, и нет необходимости использовать персональные компьютеры.

В технологии RAID существует 6 уровней для эффективного выполнения операций: RAID 0, RAID 1, RAID 3, RAID 5, RAID 10 и RAID 50. Каждый уровень RAID имеет следующие характеристики:

- *отказоустойчивость:* если один диск перестанет работать, остальные диски продолжат нормально работать;
- *производительность:* RAID имеет высокий уровень производительности при чтении и записи.

Возможность хранения данных на дисках зависит от выбора соответствующего уровня RAID. Емкость хранилища не требует, чтобы отдельные диски RAID были одинакового размера. Все уровни RAID основаны на следующих методах хранения:

- *разделение на блоки:* данные разделяются на множество блоков. Эти блоки затем записываются через систему RAID. Разделение на блоки улучшает хранение данных;

- *зеркалирование:* зеркалирование осуществляет копирование данных и регулярное сохранение их по всему RAID. Этот метод устойчив к ошибкам и имеет высокий уровень реализации;

- *контрольное значение:* контрольное значение использует функцию блокировки при выполнении функции проверки целостности блока данных. Когда диск поврежден, контрольное значение пытается восстановить данные с помощью функции исправления ошибок.

Системы RAID имеют свои преимущества и недостатки в зависимости от уровня реализации.

Преимущества систем RAID:

производительность и надежность: технология RAID увеличивает скорость чтения и записи данных на дисках. Эта технология повышает производительность за счет распределения процесса IO, а скорость процесса выше, чем при хранении данных на одном диске;

контроль ошибок: выполняет восстановление или исправление данных, хранящихся на поврежденном диске, путем сравнения их с остальными данными в диске;

избыточность данных (копирование данных): повреждение диска может произойти в любой момент. Технология RAID обеспечивает восстановление данных путем копирования их при повреждении устройства;

поочередность дисков: увеличивает производительность чтения/ записи данных. Данные разбиваются на небольшие части и распределяются по нескольким дискам. В системе RAID данные считываются и записываются одновременно;

продолжительность работы системы: это измерение определяет надежность и стабильность компьютера. Продолжительность работы системы определяет время автоматической работы системы.

Недостатки систем RAID:

написание сетевых драйверов: поскольку технология RAID в первую очередь спроектирована для использования на серверах, ее основным недостатком является то, что она записывает все сетевые драйверы;

несовместимость: системы поддерживают разные драйверы RAID. Определенный аппаратный или программный компонент может быть несовместим с системой RAID, настроенной на сервере. Несовместимость может привести к тому, что система RAID не сможет правильно выполнять свои функции;

потеря данных: драйверы RAID могут не выполнять свои функции из-за механических проблем. Риск потери данных увеличивается при последовательном повреждении дисков;

длительное время восстановления: использование дисков, больших объемов приводит к увеличению скорости передачи данных. Однако восстановление данных на дисках с большим объемом и настройка поврежденных дисков занимает много времени;

высокая стоимость: внедрение технологии RAID требует больших экономических затрат. Это также требует приобретения дополнительных контроллеров RAID и драйверов устройств, для повышения производительности системы.

Выбор подходящего уровня RAID зависит от потребностей организации и должен основываться на возможностях, предоставляемых каждым уровнем. При выборе уровня RAID требуется также обращать внимание на их характеристики (табл.6.1).

Методы резервного копирования. Организация выбирает метод резервного копирования, исходя из своих финансовых возможностей и ИТ-инфраструктуры. Существуют следующие методы резервного копирования данных:

горячее резервирование. Этот метод резервного копирования данных широко используется на практике и называется также методом динамического или активного резервного копирования. С помощью этого метода пользователь также может выполнять процесс резервного копирования во время управления системой. Реализация этого метода резервного копирования сократит время простоя системы. Изменения данных во время резервного копирования не влияют на окончательную резервную копию.

Очевидно, что при резервном копировании производительность системы замедляется.

холодное резервирование. Этот метод резервирования, также известный как оффлайн резервирование, осуществляется, когда система не работает или не управляется пользователем. Этот метод является безопасным методом резервирования и защищает от различных угроз при копировании данных.

Таблица 6.1

Анализ технологий RAID

RAID	**Использо-вание диска**	**Устойчи-вость к разруше-ниям**	**Трансфер больших данных**	**Уровень IO**	**Доступ-ность данных**	**Главный недостаток**
Еди-ный диск	Одинако-вое 100%	Нет	Хороший	Хороший	MTBF период одного диска	При повреждении диска данные теряются
RAID 0	Отличное 100%	Да	Очень хороший	Очень хороший	Низкий MTBF период диска	
RAID 1	Среднее 50%	Да	Хороший	Хороший	Хоро-ший	Использование в 2 раза меньше дискового пространства
RAID 3	Хорошее - очень хорошее	Да	Очень хороший	Хороший	Хоро-ший	При повреждении диска данные теряются
RAID 5	Хорошее - очень хорошее	Да	Хороший - очень хороший	Хороший	Хоро-ший	При повреждении диска данные теряются
RAID 0 + 1	Среднее 50%	Да	Хороший	Очень хороший	Хоро-ший	Использование в 2 раза меньше дискового пространства
RAID 1 + 0	Среднее 50%	Да	Очень хороший	Очень хороший	Очень хоро-ший	Слишком дорого, не обширно
RAID 30	Хорошее - очень хорошее	Да	Очень хороший	Отлич-ный	Отлич-ный	Слишком дорого
RAID 50	Хорошее - очень хорошее	Да	Хороший - очень хороший	Отлич-ный	Отлич-ный	Слишком дорого

Примечание: MTBF - Mean Time Between Failures (среднее время между нарушениями).

Теплое резервирование. В этом резервировании система должна быть подключена к сети для выполнения регулярных обновлений. Это важно при зеркальном отображении или копировании данных. В этом методе резервное копирование данных занимает много времени, и процесс осуществляется с определенным временным интервалом (от дней до недель).

При резервном копировании важно выбрать место для хранения данных. Резервные копии можно сохранять по следующим адресам.

Внутреннее (onsite) резервирование. Этот метод резервирования осуществляется внутри организации, которая использует внешние устройства, ленточные накопители, DVD-диски, жесткие диски и другие носители. Внутренние устройства резервирования выбираются в соответствии с объемом хранящихся данных.

Внешнее (offsite) резервирование. Внешнее резервирование может быть осуществлено в удаленном адресе, а хранение данных на физических дисках может осуществляться онлайн или через службу третьей стороны.

Резервирование в облачной системе. Этот метод резервного копирования также называется онлайн методом. Он хранит резервные копии данных в открытой сети или на определенном сервере. Как правило, определенная функция сервера может выполняться службой третьей стороны.

Типы резервирования. Подходящий тип резервирования не перегружает сеть и требует меньше затрат, времени и ресурсов. На практике существует три типа резервирования: *полное, дифференциальное* и *возрастающее***.**

Полное резервное копирование: этот метод также называется нормальным резервированием и осуществляется автоматически по графику. При этом все файлы копируются и сохраняются в укомплектованном виде. Этот метод обеспечивает эффективную защиту скопированных данных.

Возрастающее резервирование: резервирование согласно этому методу осуществляется при изменении данных, для которых выполняется резервирование. В качестве оконечного резервного копирования можно использовать любой метод резервирования.

Поэтому перед реализацией возрастающего резервирования система должна выполнить полное резервирование.

Допустим, что согласно графику резервного копирования, полное резервирование запланировано на воскресенье, а возрастающее резервирование со вторника до субботы. После того, как в воскресенье будет осуществлено полное резервирование, изменения понедельника будут внесены во вторник на основе метода возрастания. Этот процесс продолжается до субботы (рис.6.1«а»).

Дифференциальное резервирование: этот метод резервирования представляет собой совокупное представление о методах полного и возрастающего резервирования, в котором осуществляется резервное копирование изменений, сделанных из последней резервной копии.

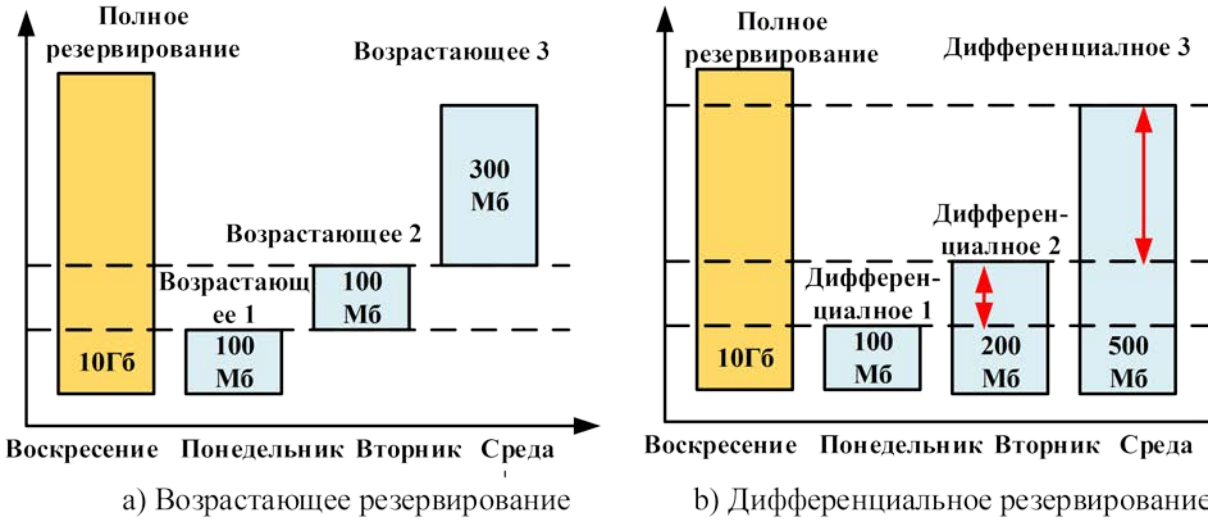


Рис.6.1. **Типы резервирования**

Рассмотрим приведенный выше пример. Пусть на графике будет указано то, что полное резервирование осуществляется в воскресенье, а дифференциальное – до субботы. После того, как полное резервное копирование будет выполнено в воскресенье, дифференциальное резервное копирование будет выполнено по истечению суток в понедельник. Эта ситуация похожа на возрастающее резервирование. Однако во вторник резервирование будет осуществляться для изменений в воскресенье и понедельник.

После этого, в среду резервирование реализуется для воскресенья, понедельника и вторника (рис. 6.1 «б»).

6.3. Восстановление данных и регистрация событий

Восстановление данных. Потеря данных является серьезной проблемой для любой организации. Поэтому требуется использование методов восстановления данных. Этот процесс зависит от способа потери данных, программного обеспечения для восстановления данных и адреса для восстановления данных.

Можно восстановить данные на носителях данных, USB-накопителях, жестких дисках, DVD и других носителях. Успех процесса восстановления зависит от квалификации пользователя. В процессе восстановления данных важными являются знания и правильно подобранное средство.

Восстановление данных не всегда может быть успешным. Если в хранилище произошла ошибка или оно сильно повреждено, восстановление данных может быть невозможным. Вероятность восстановления данных зависит от причины их потери. Случаи потери данных могут быть следующими:

удаление файла: если файл удален, эта область останется в хранилище до тех пор, пока она не будет перезаписана. Запись данных в небольшую память в области хранения данных может привести к тому, что все данные не будут восстановлены. В ОС Windows существует алгоритм удаления данных в файловой системе NTFS, и восстановление данных также выполняется на основе этого алгоритма.

повреждение файла: если ОС повреждена, данные можно восстановить с помощью таблицы разделов диска. Если таблица разделов диска также повреждена, придется воспользоваться специальными средствами восстановления.

физическое повреждение жесткого диска: физическое воздействие на жесткий диск может привести к большим потерям, чем повреждение файла. Это требует использования специального уровня восстановления данных. Во время восстановления данных с поврежденного физического диска среда процесса восстановления должна быть свободной от различных загрязнений. То есть, этот

процесс нужно производить в чистом помещении. В пыльной среде восстановление данных будет затруднено.

При восстановлении данных необходимо помнить о следующем:

- не записывать восстановленные данные на жесткий диск, где данные были потеряны;
- выполнять различные резервные копии и хранить их по разным адресам;
- восстановление данных не всегда на 100% эффективно.

На практике для восстановления потерянных данных из хранилища используются специальные программные средства. В качестве примера можно привести *Recovery My Files, EASEUS Data Recovery Wizard,* Advanced Disk Recovery, Handy Recovery, R-Studio, Data Recovery Pro, Recuva, Total Recall, Pandora Recovery.

Регистрация событий. При ошибке администратор системы или сотрудник поддержки должны выяснить причину ошибки, постараться восстановить утерянные данные и не допустить повторение ошибки. Важным является то, что приложения, операционная система и другие системные службы регистрируют важные события, например, такие как малый объем памяти или чрезмерная попытка использования диска. Администратор системы может определить причину ошибки, и, чтобы определить контекст, в котором он реализуется, использовать журнал событий (также называется лог файлом).

Регистрация событий должна включать в себя следующие события:

События операционной системы:

- запуск и отключение системы;
- начало и окончание обслуживания;
- изменения или неудачи в сетевом подключении;
- попытки изменить настройки безопасности системы и элементы управления.

Записи аудита ОС:

- попытки входа в систему (успешные или неудачные);
- функции, выполняемые после входа в систему (например, чтение или обновление важного файла, установка программы);
- изменение учетной записи (например, создать и удалить учетную запись, назначить права);

- успешное/неудачное использование привилегированной учетной записи.

Информация об учетной записи приложения:

- успешные и неудачные попытки аутентифицировать приложения;
- изменения в учетной записи (например, создание и удаление учетной записи, назначение прав учетной записи);
- использование программных привилегий.

Операции приложения:

- запуск и отключение программы;
- программные ошибки;
- основные изменения в конфигурации программы.

Зарегистрированные детали различны для каждого события, и их рекомендуется регистрировать по следующим параметрам:

- отметка времени;
- коды событий, состояний и / или ошибок;
- имя сервиса / команды / приложения;
- событие, связанное с пользователем или системой;
- текущее устройство (например, IP адрес и адрес источника, идентификатор сессии терминала, веб-браузер и т.д.).

Поскольку все действия регистрируются в журналы аудита, злоумышленники могут скрыть свои действия, редактируя их. Поэтому мониторинг использования журнала аудита является важной задачей.

Типы событий в ОС Windows. В ОС Windows регистрируются пять типов событий. Для всего этого есть четко определенные данные, а сообщение о событии будет принадлежать только одному типу (табл. 6.2).

Следующие события должны быть зарегистрированы:

проблемы ресурса. Регистрация предупреждающего события в случае ошибки выделения памяти помогает указать причину нехватки памяти;

проблемы, связанные с аппаратом. События, связанные с сетевой картой, жестким диском, оперативной памятью и другими драйверами устройств, должны быть зарегистрированы;

информационные события. Серверная программа (например, сервер базы данных) должна записывать регистрацию пользователей, операции с базой данных и другие события.

Таблица 6.2

Типы событий Windows ОТ

Событие	Описание
Ошибка	Событие, указывающее на важную проблему, такую как потеря данных или функциональности. Например, если служба не загружается при запуске, это событие ошибки регистрируется
Предупреждение	Хотя событие не имеет большого значения, оно может указывать на проблемы, которые могут возникнуть в будущем. Например, если на диске мало свободного места, регистрируется предупреждающее событие
Информация	Событие, описывающее успешную работу приложения, драйвера или службы. Например, когда сетевой диск успешно загружен, события регистрируются информацией
Успешный аудит	Событие, регистрирующее попытки доступа, связанное с успешно проверенной безопасностью. Например, успешная попытка пользователя войти в систему регистрируется как успешное событие аудита
Неудачный аудит	Это событие регистрируется, когда попытка доступа к проверенной безопасности не удалась. Например, это событие регистрируется, когда пользователю не удается войти в сетевой диск

Следующие события должны быть зарегистрированы:

Проблемы ресурса. Регистрация предупреждающего события в случае ошибки выделения памяти помогает указать причину нехватки памяти.

Проблемы, связанные с аппаратом. События, связанные с сетевой картой, жестким диском, оперативной памятью и другими драйверами устройств, должны быть зарегистрированы.

Информационные события. Серверная программа (например, сервер базы данных) должна записывать регистрацию пользователей, операции с базой данных и другие события.

Над журналом событий можно выполнять следующие операции:

– резервное копирование (с помощью функции Backup Event Log);

– очистка (с помощью функции Clear Event Log);

– мониторинг (с помощью функции Notify Change Event Log);

– отправка запроса (другими программами, с помощью функции Get Oldest Event Log Record, Get Number Of Event Log Records);

– чтение (с помощью функции Read Event Log);

– запись (с помощью функции Report Event).

В операционных системах Windows XP/2000 журнал регистрации событий имеет привилегии, предоставленные различным учетным записям (табл. 6.3).

Таблица 6.3

Привилегии, доступные в журнале событий в ОС Windows XP/2000

Лог	Учетная запись	Чтение	Запись	Очистка
Относительно приложения	Администраторы (система)	+	+	+
	Администраторы (домен)	+	+	+
	Локальная система	+	+	+
	Интерактивный пользователь	+	+	-
Относительно системы	Администраторы (система)	+	+	+
	Администраторы (домен)	+	-	+
	Локальная система	+	+	+
	Интерактивный пользователь	+	-	-
Лог файл, созданный на основе выбора	Администраторы (система)	+	+	+
	Администраторы (домен)	+	+	+
	Локальная система	+	+	+
	Интерактивный пользователь	+	+	-

Для просмотра файлов регистрации событий (лог файла) в ОС Windows выполняется следующая последовательность:

1. В компьютере нажимается комбинация клавиш Win + R.
2. В *появившемся* поле вводится *eventvwr* и нажимается кнопка Enter.
3. В появившемся окне просмотра событий выбирается пункт *Windows Logs* (рис. 6.2).

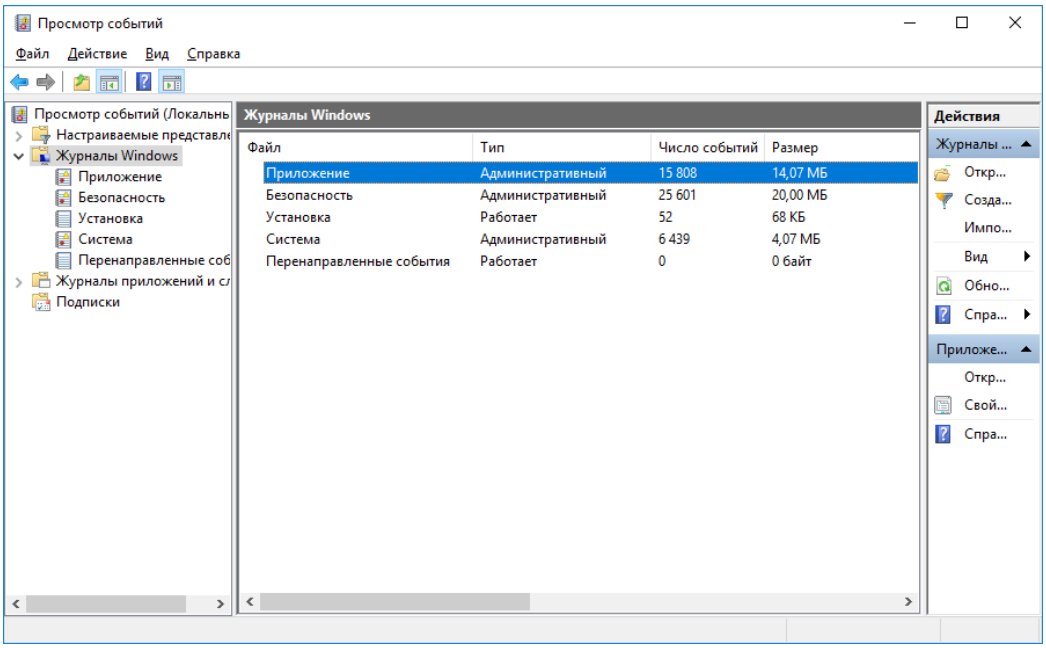


Рис.6.2. **Окно журнала событий ОС Windows**

Контрольные вопросы

1. Понятие доступности и ее важность для системы.
2. Резервное копирование и его виды.
3. Основные причины, приводящие к потере данных.
4. Последовательность задач, выполняемых при резервном копировании.
5. Устройства хранения резервных копий и их особенности.
6. Технология RAID и ее основные особенности.
7. Типы резервирования, их преимущества и недостатки.

ГЛАВА 7. БЕЗОПАСНОСТЬ ПРОГРАММНЫХ СРЕДСТВ

7.1. Проблемы безопасности в программных средствах

В настоящее время безопасность программных средств является важной областью информационной безопасности, такой как криптография, контроль доступа и протоколы безопасности. Причина в том, что виртуальная безопасность информации достигается с помощью программных средств. В случае если программное средство окажется под угрозой, механизм безопасности также выйдет из строя.

Во всех программных средствах имеются уязвимости, уровни которых различаются. Например, NASA Mars Lander, цена которого составляет 165 млн. $, потерпел крушение при приземлении на поверхность Марса. Это произошло из-за разницы между обычным английским и международным измерением метровой длины. Кроме того, в результате недостатков в программном средстве, используемых в системе управления грузами в международном аэропорту Денвера, в день был нанесен ущерб в размере 1 млн. $ в течение 11 месяцев.

В последние годы количество и уровень серьезности этих проблем уязвимости увеличиваются. В частности, на рис. 7.1 показано увеличение различных уровней уязвимостей на веб-сайтах со стороны организации Positive Technologies за последние годы.

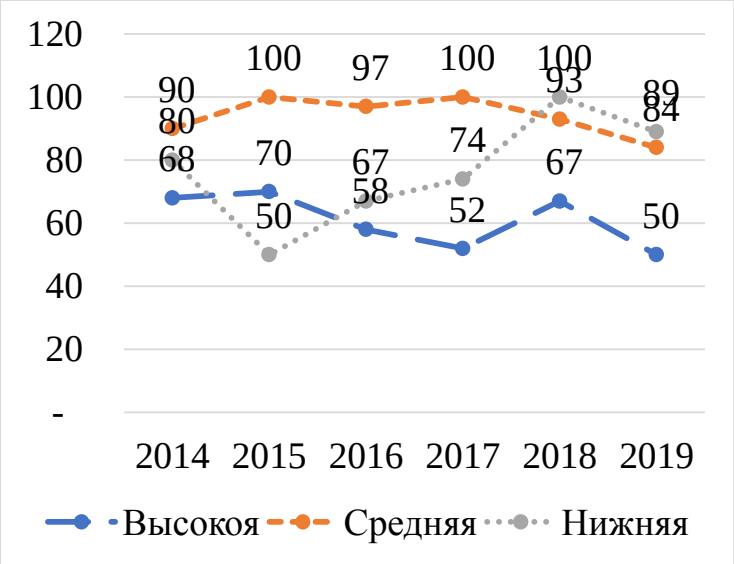


Рис.7.1. **Количество веб-сайтов с разным уровнем уязвимости**

Распределение по серьезности проблем на выявленных веб-сайтах в 2019 году показано на рис. 7.2.

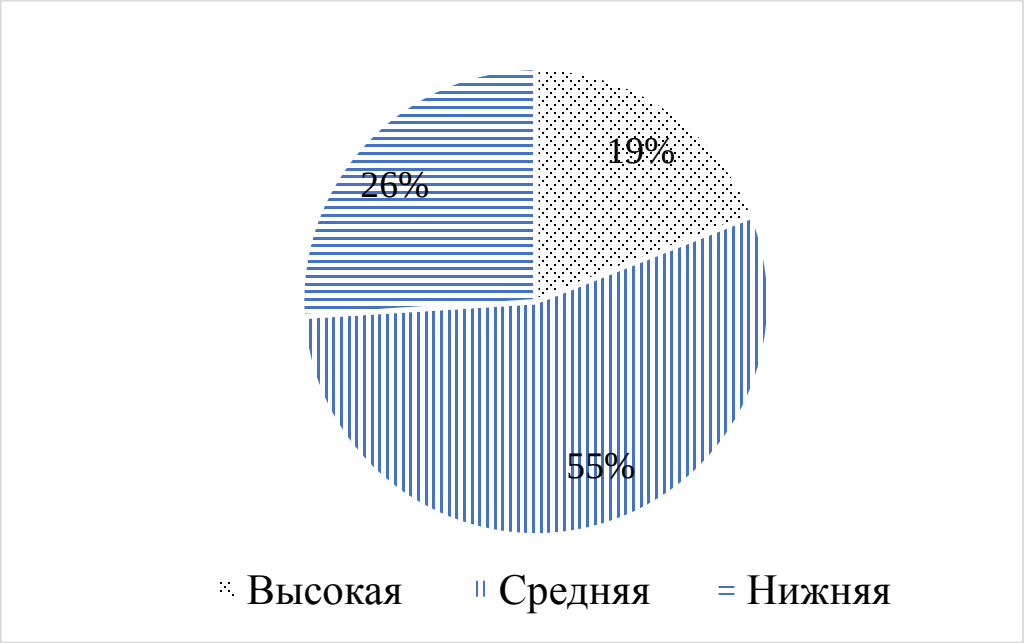


Рис.7.2. **Распределение по серьезности проблем на веб-сайте**

Согласно данным, предоставленным OWASP (Open Web Application Security Project), наиболее распространенные уязвимости на веб-сайтах в 2019 году, и их доля были следующими (рис. 7.3).

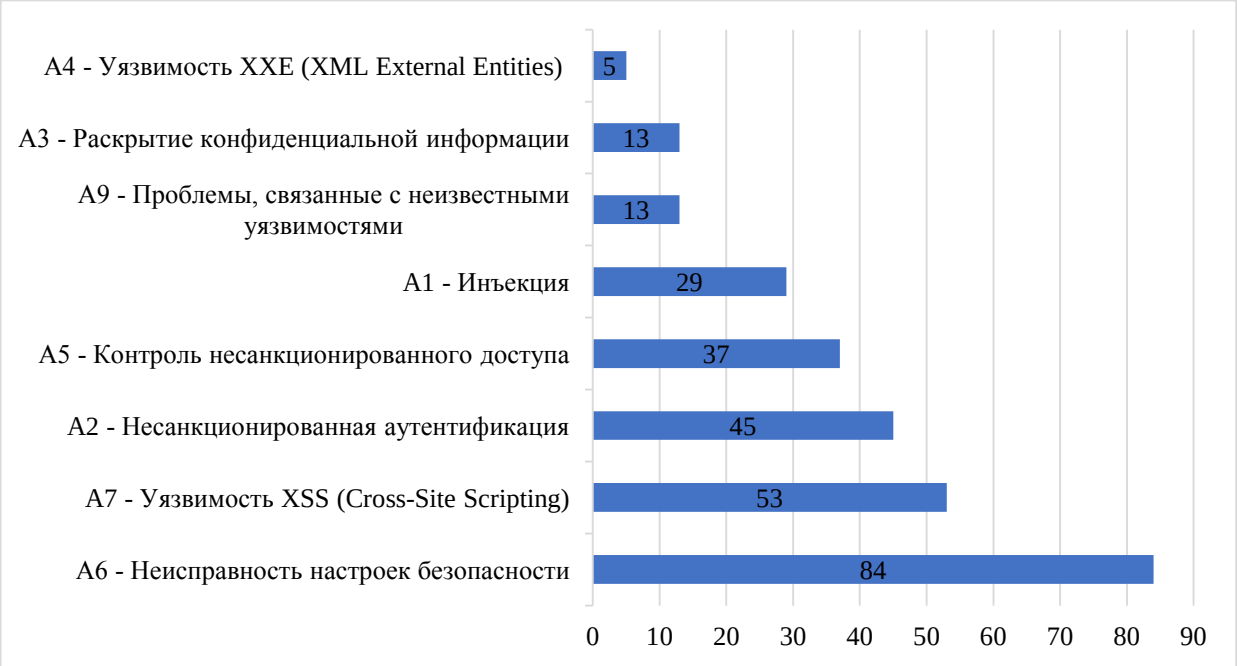


Рис.7.3. **Уязвимости, с которыми столкнулся OWASP в 2019 году, и их доля**

В результате вышеперечисленных уязвимостей, основной целью атакующих был захват различной информации (рис. 7.4).

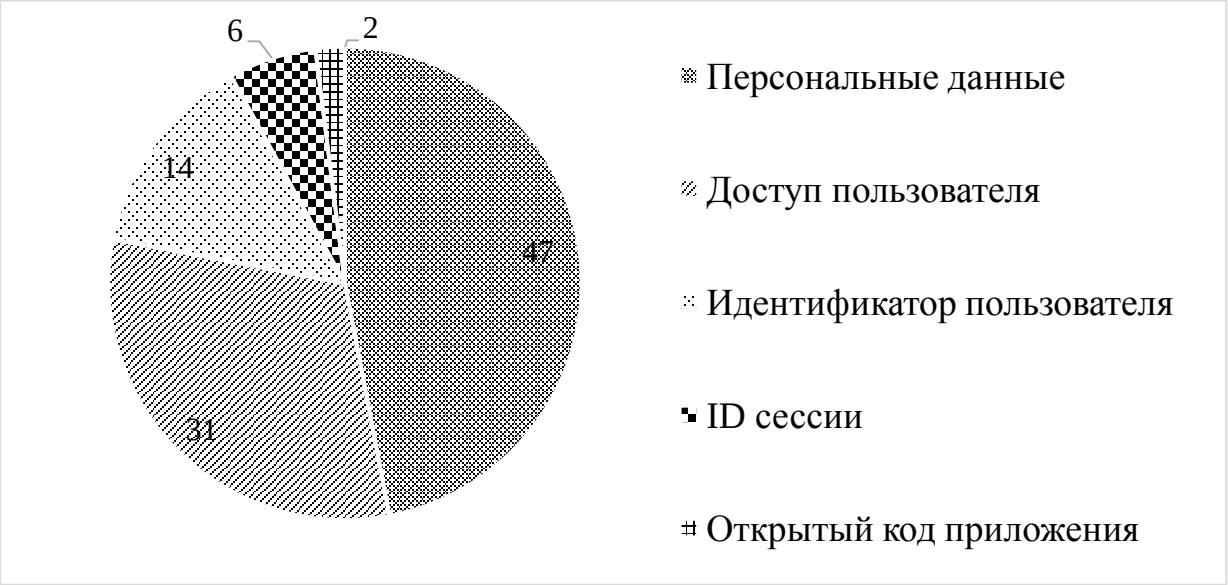


Рис.7.4. **Информация, предназначенная для получения в результате уязвимостей**

Существующие угрозы в программных средствах обычно определяются возможностями языков программирования. Например, поскольку относительно низкоуровневые языки программирования требуют от программиста высокой квалификации, у них возникают много проблем с безопасностью. Поскольку многие проблемы в языках программирования C # и Java автоматически обнаруживаются в процессе компиляции, они считаются более безопасными, чем языки программирования C или C ++.

Обычно вредоносные программные средства делятся на два типа:

- уязвимости в программах (не созданные специально);
- вредоносные программы (специально созданные).

Если первый тип – пример проблем с программами в результате ошибки, допущенной программистом, то второй тип – пример специальных программных продуктов (например, вирусов), написанных с целью нарушения.

Наличие проблем безопасности в программных средствах определяется следующими факторами:

- разработка программного обеспечения многими программистами (комплексность);
- человеческий фактор в разработке программных продуктов;
- низкая квалификация программиста;
- незащищенность языков программирования.

Тот факт, что программные средства состоят из нескольких миллионов наборов кода, это является причиной увеличения проблемы безопасности (табл.7.1). Другими словами, крупномасштабные программные средства пишутся многими программистами и под конец объединяются. Недостаточное знание одного из программистов может свести на нет безопасность всего программного средства.

Таблица 7.1

Система	**Длина кода в программе**
Netscape	17 млн.
Space Shuttle	10 млн.
Linuxkernel 2.6.0	5 млн.
Windows XP	40 млн.
Mac OS X 10.4	86 млн.
Boeing 777	7 млн.

Результаты анализа показывают, что на каждой 10 000 строке кода имеется 5 багов. Другими словами, в среднем файле .exe размером 3 Кбайт имеется до 50 багов.

Если в инженерии программных средств, программа должна гарантированно выполнять свои функции, то инженерии безопасных программных средств, требуется выполнение своих задач безопасно. Однако на практике получить полностью безопасное программное средство невозможно.

Существуют следующие понятия, связанные с уязвимостями в программных продуктах.

Дефект. Все уязвимости в реализации и проектировании программы являются дефектами, и его наличие в программных средствах может оставаться незамеченным в течение многих лет.

Баг. Баги – проблема, связанная с этапом реализации программного обеспечения, и их можно легко выявить. В качестве примера можно привести состояние *переполнения буфера* (Buffer overflow) *при* программировании.

Переполнение памяти. Часто встречающиеся на практике недостатки языков программирования обычно являются результатом ввода данных в запрещенном формате или размере. Самая распространенная из этих угроз – угроза переполнения памяти.

Например, если пользователю требуется ввести информацию на веб-сайт (имя, фамилия, год и т.д.), информация, введенная пользователем в поле «имя», записывается в поле размером с символом N на сервере. Если введенные данные превышают длину N, происходит событие переполнения памяти.

Если со стороны взломщика вводится «необходимая» ему информация, это, в свою очередь, приводит к повреждению компьютера.

Ниже приведен код, написанный на языке программирования C, если этот код компилируется, происходит событие переполнения памяти.

```
int main()
{
int buffer [10];
buffer [20] =37;
}
```

Проблема, которая существует здесь, заключается в том, что 20 байт данных записываются в 10 байт памяти. Это, в свою очередь, также становится причиной обращения к неавторизованному адресу памяти.

7.2. Фундаментальные принципы безопасности программных средств

При создании и использовании программного обеспечения требуется соблюдение ряда принципов. Ниже приведены принципы, предоставленные организацией OWASP:

Минимизация площади области, которую можно атаковать. Каждая функция, добавленная в программное обеспечение, также увеличивает уровень риска для программного обеспечения. Цель безопасной реализации программы – снизить риск в программе в целом за счет сужения области, которая может быть атакована. Например, на веб-сайтах есть функция поиска для реализации

онлайн помощи. Однако этот вариант может привести к возможности атаки на веб-сайт с помощью SQL-инъекции. Если возможность поиска предназначена для аутентифицированных пользователей, вероятность атаки уменьшается. Если поисковые данные проверяются централизованно, вероятность этой атаки еще больше снижается.

Установка безопасных стандартных настроек. На практике большинство настроек безопасности в большинстве программных обеспечений и операционных систем установлены в стандартном порядке. Однако это не очень хорошо воспринимается пользователями, и поэтому в большинстве случаев эти настройки отключаются. Например, в операционных системах время истечения срока действия пароля установлено по умолчанию, но этот параметр отключен большинством пользователей.

Принцип минимальных привилегий. Принцип минимальных привилегий, широко используемый в информационной безопасности, информатике, программировании и других областях (Principle of least privilege) – организация доступа к ресурсам на определенном уровне абстракции в вычислительной среде. Соответственно, требуется минимальное использование ресурса или информации, необходимое каждому модулю для выполнения своей функции.

Этот принцип означает, что пользователь или программист должен иметь только те привилегии, которые необходимы для его задачи. Например, различные мобильные игровые программы, предназначенные для того, чтобы скоротать время, не должны уметь читать SMS-сообщение или знать список звонящих абонентов. Например, в языках программирования для ограничения доступа к объектам (перечисленных в языке программирования Java) используются разные ключевые слова (табл. 7.2).

Если правильно разработанный интерфейс администратора правильно следует правилам использования сети, проверяет авторизацию пользователей и регистрирует все случаи, то он не может быть не устойчивым к анонимной атаке.

Нарушение безопасности. Приложения могут прерываться в процессе реализации по разным причинам. Например, ниже приведена ситуация с безопасностью, которая была оставлена без внимания.

```
isAdmin = true;
try {
  codeWhichMayFail();
  isAdmin = isUserInRole( “Administrator” );
}
catch (Exception ex) {
  log.write(ex.toString());
}
```

Таблица 7.2

Пользовательские привилегии на языке программирования Java

Привилегие / Свойство	Default	Private	Protected	Public
Одинаковый класс	+	+	+	+
Подкласс одного пакета	+	-	+	+
Не имеется подкласс одного пакета	+	-	+	+
Различные подклассы пакетов	-	-	+	+
Не имеются различные подклассы пакетов	-	-	-	+

В этом случае, если в функциях codeWhichMayFail либо в случае наблюдения Exception, пользователь будет оставаться в роли администратора. Как правило, это является риском безопасности.

Не доверчивость к сервисам. В настоящее время, многие организации используют возможности вычисления третьей партнерской организации. Например, организация может обрабатывать свои данные с помощью программного обеспечения, принадлежащего партнеру. В этом случае доверие к ним не гарантируется. Например, Payme или подобные приложения предоставляют информацию о нескольких банковских картах. В этом случае каждый банк должен проверить, правильно ли отражены его данные на стороне пользователя.

Разделение задач. Разделение задач является основной мерой, направленой на предотвращение мошенничества. Например, запрос на компьютер от организации не должен приниматься человеком, который его отправил. Причина в том, что в этом случае он может

запросить много компьютеров и отрицать их получение. В некоторых случаях уровень доверия к роли будет отличаться по сравнению с обычными пользователями. Например, администраторы должны иметь возможность отключать или включать систему, устанавливать политику паролей. Однако они не должны иметь доступ к онлайн магазину как привилегированный пользователь, в частности, они не должны иметь возможности покупать товары от имени других.

Защита безопасности от неопределенности. Безопасность, основанная на неопределенности, – это слабая защита, которая дает сбой при первой проверке. Хотя это не означает, что хранить секреты – плохая идея, это означает, что важные аспекты безопасности не основаны на секретности деталей.

Например, безопасность программы не должна давать сбоев, если известно о ее открытом коде. Безопасность должна зависеть от многих других факторов, таких как разумная политика паролей, сетевая архитектура и средства управления аудитом.

Практическим примером этого является операционная система Linux. Хотя код этой операционной системы считается открытым, он должным образом защищен и поэтому является одной из самых надежных операционных систем на сегодняшний день.

Простое обеспечение безопасности. Площадь зоны атаки и простота взаимосвязаны. Некоторые инженеры программного обеспечения предпочитают сложность кода его простому внешнему виду. Однако простой, и понятный вид может быть быстрым. Поэтому важно избегать сложностей в процессе создания программного обеспечения.

Требования безопасности к программным продуктам. При разработке программного обеспечения к нему предъявляется множество требований.

Требования к программным продуктам делятся на три типа:

- *функциональные требования:*
  - задачи, необходимые при реализации системы;
- *нефункциональные требования:*
  - требования к характеристикам системы.

Функциональные требования. Эти требования включают в себя:

– системные требования к ожидаемому доступу;

– требования к результату системы;

– входные и выходные требования.

Нефункциональные требования. К нефункциональным требованиям относятся:

– возможность проведения аудита;
– возможность расширения;
– удобства использования;
– выполняемость;
– компактность;
– надежность;
– безопасность;
– возможность тестирования;
– доступность и др.

К требованиям частной безопасности относятся:

- *Пример требования конфиденциальности:*
  - система должна отображать файлы .doc только авторизованному пользователю;
  - использовать безопасный канал связи.
- *Пример требования контроля доступа:*
  - система должна требовать использования пароля;
  - права доступа на основе ролей должны контролироваться.
- *Пример требования целостности:*
  - предоставление доступа для пользователей открытого (public) типа разрешено только чтение, для пользователей секретного (private) типа – также чтение и запись.
- *Пример требования доступности:*
  - все учетные записи должны иметь пароль;
  - учетную запись необходимо заблокировать после 3-х неудачных попыток;
  - если угроза к учетной записи не реализована в течение 5 минут, ее необходимо разблокировать.

Безопасность, основанная на языке программирования. Различные языки программирования обладают своими уникальными возможностями, поэтому обеспечение безопасности на уровне программирования имеет большое значение. Разделение существующих языков программирования на безопасные и небезопасные типы является относительным понятием, которое можно описать следующим образом (рис. 7.5).

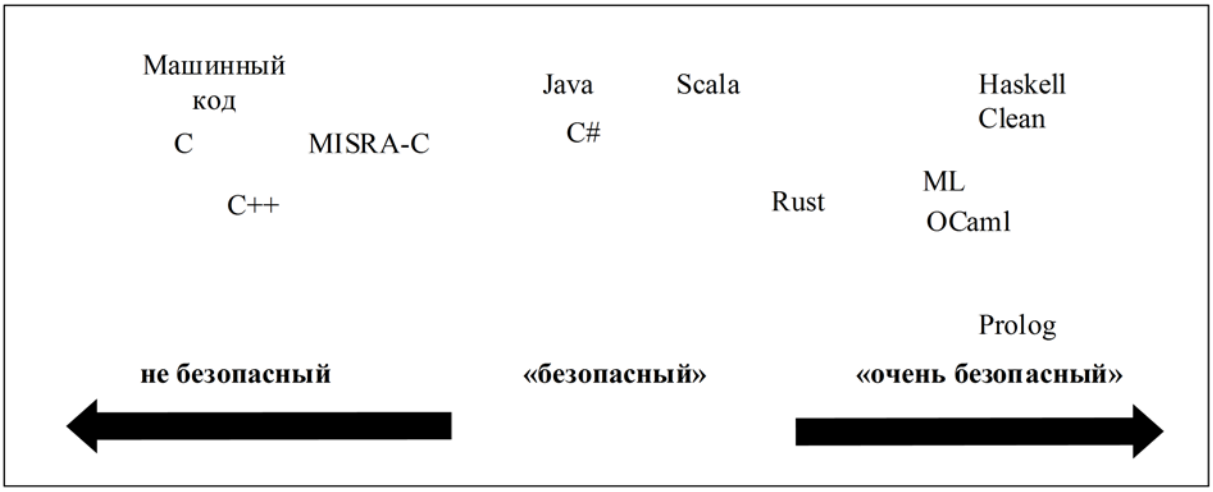


Рис.7.5. **Простой вид уровня безопасности языков программирования**

7.3. Компьютерные вирусы и проблемы защиты от вирусов

Есть много определений компьютерного вируса. Первое определение было дано Фредом Коэном в 1984 году: «Компьютерный вирус – вредоносная программа, которая заражает другие программы, вводя в них себя или модифицированную копию, изменяя их, где включенная в него программа сохраняет способность к дальнейшему воспроизведению». Способность вируса размножаться самостоятельно и модифицировать вычислительный процесс считается базовым понятием в этом определении. Эти особенности компьютерного вируса схожи с паразитированием биологических вирусов в живых организмах.

В настоящее время, под компьютерным вирусом понимается программный код, который имеет следующие особенности:

- возможность создавать копии, которые не обязательно должны соответствовать оригиналу, но имеют характеристики оригинала (самовосстановление);
- наличие механизмов, обеспечивающих включение созданных копий в исполняемые объекты вычислительной системы.

Следует отметить, что эти особенности необходимы, но их недостаточно. Эти особенности должны быть дополнены деструктивными и не разглашающими свойствами вредоносного программного воздействия в вычислительной среде.

Вирусы можно классифицировать по следующим основным симптомам:

- среда обитания;
- операционная система;
- особенности алгоритма работы;
- деструктивные возможности.

Классификация компьютерных вирусов по среде обитания, то есть по типу объектов компьютерной системы, в которые они занесены, является основной и общепринятой (рис. 7.6).

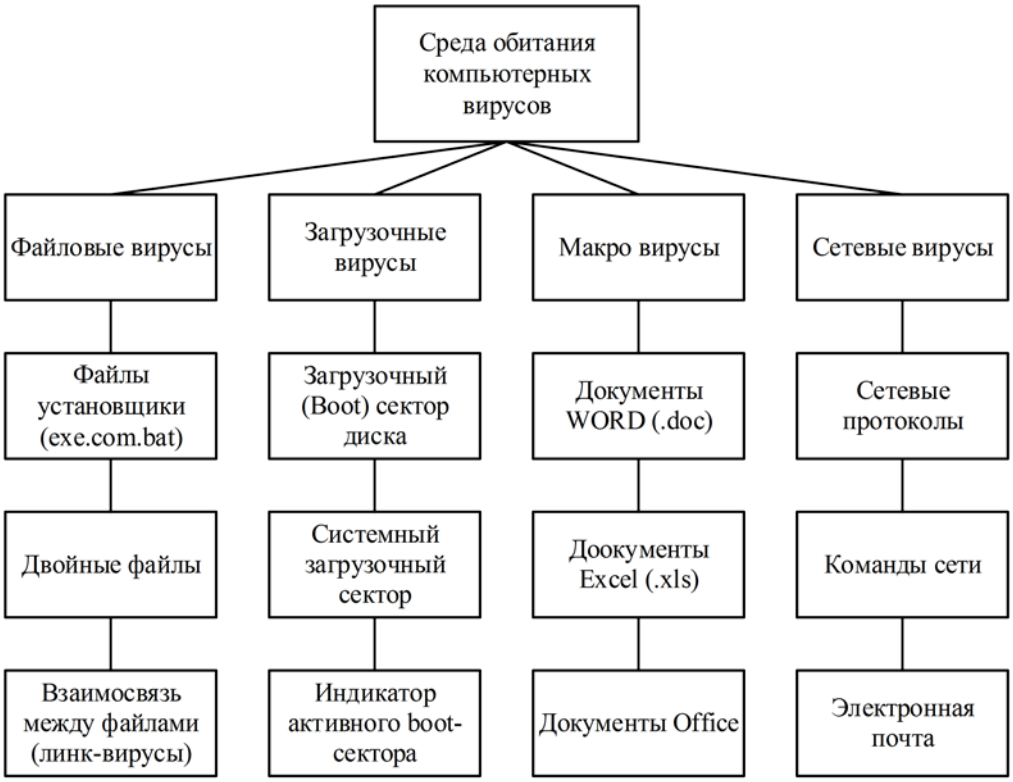


Рис.7.6. **Классификация компьютерных вирусов по среде обитания**

Файловые вирусы внедряются в исполняемые файлы различными способами (наиболее распространенный тип вирусов), создают файлы-компаньоны (вирусы-компаньоны), или используют возможность настройки файловых систем (link-вирусы).

Загрузочные вирусы записывают в загрузочный сектор диска (boot - сектор) или в сектор с загрузчиком системы винчестера (MasterBootRecord). Загружаемый вирус действует как программный код, управляющий загрузкой системы.

Макровирусы заражают макросы и файлы современных систем обработки информации, отравляют файловые документы и

электронные таблицы массовых редакторов, таких как MicroSoftWord, MicroSoftExcel и т.д.

Сетевые вирусы для распространения используют компьютерные сети, почтовые протоколы и команды. Сетевые вирусы иногда называют программами типа «червь». Сетевые вирусы делятся на интернет-червей (распространяются через Интернет), IRC-червей (чаты, InternetRelayChat).

Также существует множество комбинаций компьютерных вирусов, таких как сетевой макровирус, который заражает редактируемые документы и распространяет свои копии по электронной почте. В качестве другого примера можно привести вирусы, загружающие файлы, которые заражают файлы и загрузочный сектор дисков.

Жизненный цикл вирусов. Как и в любой программе, компьютерные вирусы можно разделить на два основных этапа жизненного цикла – этапы хранения и выполнения.

Этап хранения соответствует периоду хранения вируса на диске вместе с объектом, в который он вставлен. На этом этапе вирус становится уязвимым для антивирусного программного обеспечения, поскольку он неактивен и не может контролировать операционную систему для защиты.

Период выполнения компьютерных вирусов обычно включает в себя пять этапов:

1. Загрузка вируса в память.
2. Поиск жертвы.
3. Заражение найденной жертвы.
4. Выполнение деструктивных функций.
5. Передача управления вирусной программе-носителю.

Загрузка вируса в память. Загрузка вируса в память осуществляется одновременно с исполняемым объектом, куда вирус вставляется с помощью операционной системы. Например, если пользователь запускает программный файл, содержащий вирус, очевидно, что код вируса загружается в память как часть этого файла. Обычно процесс загрузки вируса – копирование с диска в оперативную память, а затем управление передается коду тела вируса. Эти действия выполняет операционная система, сам вирус находится в пассивном состоянии. В более сложных задачах вирус может выполнять дополнительные действия для своей

работы после взятия контроля. Рассматриваются два аспекта, связанные с этим.

Первый связан с максимальной сложностью процедуры обнаружения вирусов. На этапе хранения некоторые вирусы используют достаточно сложный алгоритм для обеспечения защиты. К такому усложнению можно отнести шифрование основной части вируса. Однако использование только шифрования является неполной мерой, так как на этапе загрузки та часть вируса, которая обеспечивает расшифровку, должна храниться в открытом виде. Чтобы избавиться от этой ситуации, разработчики вирусов используют механизм «мутации» расшифрующего кода. Суть этого метода заключается в том, что при введении вирусной копии в объект соответствующая часть его расшифровки модифицируется таким образом, что появляется текстовое различие с оригиналом, но результат работы не меняется.

Вирусы, использующие механизм мутации кода, называются *полиморфными вирусами*. Полиморфные вирусы (polymorphic) – трудно вычисляемые вирусы, у которых нет сигнатур, то есть они не содержат постоянной части кода. Полиморфизм встречается в файловых, загружаемых и макровирусах.

При использовании стелс-алгоритмов вирусы могут полностью или частично скрывать себя в системе. Вирусы, использующие стелс-алгоритмы, называются *стелс-вирусами* (Stealth). Вирусы Стелс маскируют свою среду обитания, перехватывая доступ операционной системы к поврежденным файлам и перенаправляя операционную систему на неповрежденную часть информации.

Второй аспект связан с вирусами, называемыми *вирусами резидентами*. Поскольку вирус и объект, в который он входит, являются неотъемлемой частью операционной системы, после загрузки они, естественно, будут располагаться в одном адресном пространстве. Когда объект закончен, он освобождается из оперативной памяти. При этом в то же время вирус высвобождается и переходит в пассивную фазу хранения. Однако некоторые вирусы могут сохраняться в памяти и оставаться активными после завершения работы вирусоносителя. Такие вирусы получили название резидента. Вирусы резиденты обычно заражают среду обитания, используя только привилегированные режимы, разрешенные операционной системой, и действуют как вредители при определенных условиях. Вирусы резиденты

располагаются в памяти и остаются активными до выключения компьютера или перезапуска операционной системы.

Нерезидентные вирусы выполняют функции заражения и вредительства, попав в память, только когда они активированы. Затем эти вирусы полностью покидают память и остаются в среде обитания.

Следует отметить, что разделение вирусов на резидентные и нерезидентные распространяется только на файловые вирусы. Загрузчики и макровирусы относятся к резидентным вирусам.

Поиск жертвы. Вирусы делятся на два класса по методу поиска жертвы. К первому классу относятся вирусы, выполняющие активный поиск с использованием функций операционной системы. Ко второму классу относятся вирусы, выполняющие пассивные поисковые системы, то есть вирусы, ставят ловушки в программных файлах.

Заражение найденной жертвы. Обычно под заражением понимается самокопирование вирусного кода на объект, выбранный в качестве жертвы.

Сначала посмотрим на свойства заражения файловых вирусов. В ней различаются вирусы двух классов. Вирусы первого класса не вводят свой код непосредственно в файл программы, а изменяют имя файла и создают новый файл, который является телом вируса. Ко второму классу относятся вирусы, которые проникают непосредственно в файлы жертвы. Эти вирусы характеризуются местами проникновения. Возможны следующие варианты:

1. *Ввод в начала файла.* Этот метод является наиболее удобным для com-файлов MS-DOS, поскольку в этом формате предусмотрены служебные заголовки.
2. *Ввод в конец файла.* Этот метод является наиболее распространенным, и передача управления коду вируса обеспечивается изменением первой команды программы (*com*) или заголовка файла (*exe*).
3. *Ввод в середину файла.* Обычно этот метод используется для применения структуры вирусов к заранее определенным файлам (например, файлу *Command.com*) или к файлам, содержащим последовательность байтов одного и того же значения, достаточно длинную, чтобы вместить вирус.

Характеристики этапа заражения для загрузочных вирусов определяются качеством загрузочных секторов объектов, в которые

они вставлены – гибких и жестких дисков, а также загрузочной записи жесткого диска (MBR). Основная проблема – ограниченные размеры этого объекта. Следовательно, вирусы должны хранить на диске неподходящую часть своей жертвы, а также нести оригинальный код зараженного загрузчика.

Процесс заражения для макровирусов заключается в хранении кода вируса в выбранном документе жертвы. Это непросто сделать для некоторых программ обработки информации, поскольку формат файла документа может быть не предназначен для хранения макропрограмм.

Выполнение деструктивных функций. По деструктивным возможностям различаются безвредные, безопасные, опасные и очень опасные вирусы.

Безвредные вирусы – вирусы, обладающие механизмом самораспространения. Они не повреждают систему, только занимают свободное место на диске.

Безопасные вирусы – вирусы, связанные с различными впечатлениями (аудио, видео) от присутствия в системе, не наносят ущерба программам и данным, хотя и сокращают свободную память.

Опасные вирусы – вирусы, вызывающие серьезные дефекты в работе компьютера. В результате программное обеспечение и данные могут быть повреждены.

Очень опасные вирусы – вирусы, которые внедряются в алгоритмы предварительной обработки их обработки, приводя непосредственно к уничтожению программ и данных, а также удалению информации, необходимой для работы компьютера.

Передача управления программе – носителю вируса. Следует отметить, что вирусы делятся на разрушителей и не разрушителей.

Разрушительные вирусы не заботятся о сохранении функциональности при заражении программ, поэтому на данном этапе они не имеют смысла.

Для *не разрушительных вирусов* этот этап связан с восстановлением и управлением программой в памяти в том виде, в котором необходимо выполнить корректировку, переместив вирус к программе-носителю.

Другие типы вредоносных программ. Помимо вирусов, существуют следующие типы вредоносных программ:

- троянские программы;

- логические бомбы;
- хакерские утилиты, которые тайно управляют удаленными компьютерами;
- программы, которые воруют пароли из Интернета и с другой конфиденциальной информации.

Между ними нет четкой границы: троянские программы могут содержать вирусы, логические бомбы могут быть размещены на вирусах и т.д.

Троянские программы не воспроизводятся и не распространяются. Со стороны троянские программы выглядят абсолютно безобидными, даже рекомендуют полезные функции. Однако если пользователь загружает и запускает такую программу на своем компьютере, программа может выполнять вредные функции не заметно. Большинство троянских программ используются для первоначального распространения вирусов, использования удаленного компьютера через Интернет, кражи данных или их удаления.

Логическая бомба – это программа или отдельные ее модули, выполняющие вредоносные действия при определенных условиях. Логическая бомба, может быть запущена, например, когда наступает определенная дата, или, когда запись появляется или исчезает в базе данных, и т.д. Такую бомбу можно установить на вирусы, троянские программы и простые программы.

Каналы распространения вирусов и вредоносных программ. Для создания эффективной системы защиты компьютеров и корпоративных сетей важно иметь четкое представление о том, откуда исходит угроза. Вирусы находят самые разные каналы распространения. Кроме того, к старым методам добавляются новые.

Классические методы распространения. Файловые вирусы распространяются вместе с файлами программ при обмене дискетами и программами, загрузке программ из сетевых каталогов, Web- или FTP-серверов. Загрузочные вирусы попадают на компьютер, когда пользователь оставляет зараженную дискету на дисководе, а затем перезагружает операционную систему. Загружаемый вирус может проникнуть в компьютер через другие типы вирусов. Вирусы макрокоманд распространяются через обмен зараженными файлами офисных документов, таких как файлы MicroSoftWord, Excel, Access.

Если зараженный компьютер подключен к локальной сети, вирус может легко заразить диски файлового сервера, откуда он может пройти через каталоги на все компьютеры в сети. Таким образом, начинается вирусная эпидемия. Системный администратор должен помнить, что вирус имеет те же права в сети, что и права пользователя компьютера, который был заражен. Таким образом, он может попасть во все каталоги, которые использует пользователь. Если вирус попадает на рабочую станцию администратора сети, последствия могут быть очень плачевными.

Электронная почта. В настоящее время основным источником вирусов является глобальная сеть Интернет. Большинство вирусных заражений происходит при обмене письмами в формате MicroSoftWord. Электронная почта служит каналом для передачи макровирусов, поскольку вместе с информацией часто отправляются офисные документы.

Отравление вирусами может происходить бессознательно и со злым умыслом. Например, пользователь редактора, зараженного макровирусом, может сам того не подозревая отправлять отравленные электронные письма адресатам. С другой стороны, злоумышленник может намеренно отправить любой опасный программный код по электронной почте.

Троянские Web-сайты. Пользователи могут получить вирус или троянскую программу при простом отслеживании, просмотре троянских *Web*-сайтов. Ошибки в пользовательских браузерах часто становятся причиной того, что активные компоненты троянских *Web*-сайтов вводят вредоносную программу на компьютеры пользователей. Пользователь может получить приглашение для просмотра сайта троянца по простой электронной почте.

Локальные сети. Локальные сети также являются средством быстрого заражения. Если необходимые меры защиты не приняты, зараженная рабочая станция отравит один или несколько служебных файлов на сервер при доступе к локальной сети. К таким файлам можно отнести служебный файл Login.com, электронные таблицы Excel, используемые организацией, и стандартные шаблоны документов. При входе в эту сеть пользователи запускают зараженные файлы с сервера, в результате чего вирус получает доступ к компьютеру пользователя.

Другие каналы распространения вредоносных программ. Один из каналов распространения вирусов – пиратские копии программного обеспечения. Нелегальные копии дискет и компакт-дисков часто содержат файлы, зараженные различными вирусами. К источникам передачи вируса также относятся электронные конференции и файловые серверы FTP и BBS.

Компьютеры, установленные в учебных заведениях и Интернет-центрах и работающие в общедоступном режиме, также легко могут стать источником распространения вирусов. Если один из этих компьютеров отравлен дискетой следующего пользователя, дискеты других пользователей, работающих на этом компьютере, также будут отравлены.

С развитием компьютерных технологий компьютерные вирусы также усовершенствуются по мере их адаптации к новой среде обитания. В любой момент могут появиться новые, ранее неизвестные или известные компьютерные вирусы, разработанные для нового компьютерного оборудования, троянские программы и черви. Новые вирусы могут использовать неизвестные или ранее не существовавшие каналы распространения, а также новые технологии для внедрения в компьютерные системы. Чтобы исключить риск заражения вирусом, системный администратор корпоративной сети должен не только использовать антивирусные методы, но и постоянно следить за миром компьютерных вирусов.

Обнаружение вредных программных средств. В основном используются три подхода к обнаружению вредоносных программ. Первым и наиболее распространенным их них является *обнаружение на основе сигнатур,* основанное на поиске шаблона или сигнатуры во вредоносной программе. Второй подход основан на *обнаружении изменений* и выявляет файлы, которые подверглись изменению. Когда файл неожиданно подвергается изменению, то он считается зараженным. Третий подход *основан на аномалиях*, и выявляет непривычных или вирусных файлов и ситуаций.

Обнаружение на основе сигнатур. Сигнатура – последовательность обнаруженных битов в файле, содержащая специальные символы. В этом случае их хэш-значения также могут служить в качестве сигнатуры. Однако этот метод имеет низкий уровень гибкости, и вирусописатели могут легко его обойти.

Например, сигнатура 83EB 0274 EBOE 740A 81EB 0301 0000 была использована для вируса W32 / Beast (вирус, обнаруженный в 1999 году и предназначенный для заражения документа Microsoft Word). В этом случае ведется поиск данной сигнатуры во всех файлах в системе. Однако нельзя сказать с уверенностью, что вирус обнаружен полностью, даже если эта сигнатура была обнаружена в файле. Это потому, что невирусный файл также может содержать данную сигнатуру. Если биты, подлежащие поиску файлов случайны, потенциальная вероятность заражения равна $1/2^{112}$. Однако компьютерные программы и биты в данных далеки от случайности, и это означает, что вероятность все больше возрастет. Другими словами, даже в случае обнаружения в определенном файле сигнатуры, требуется дополнительная проверка.

Метод обнаружения на основе сигнатуры очень эффективен в случае, когда вирус действительно существует и общие сигнатуры разделены. Кроме того, согласно этому методу пользователю и администратору накладывается минимальная нагрузка и возлагается на них только задача хранения сигнатур и их постоянное обновление.

Однако, размер файла, в котором хранятся сигнатуры, велик, и сканирование с использованием файла с 10 или 100 тысячами сигнатурами занимает много времени. Кроме того, этот метод можно легко обмануть с помощью небольшой модификации обнаруженного вируса.

На сегодняшний день метод распознавания на основе сигнатур широко используется в современных антивирусах или средствах защиты от вредоносных программ.

Метод обнаружения изменений. Поскольку вредоносная программа находится по определенному адресу, то можно указать на зараженность, если где-то в системе обнаружено изменение. То есть, если обнаружен измененный файл, он может быть заражен вирусом.

Как можно обнаружить изменения? Для решения этой проблемы подходят хэш-функции. Предположим, что все файлы в системе хэшированы, а хэш-значения хранятся в безопасном месте. В этом случае время от времени хэш-значения этого файла повторно вычисляются и сравниваются с исходным значением.

Если один или несколько битов файла изменены, хэш-значения не совпадут, и файл считается зараженным вирусом.

Одним из преимуществ этого метода является то, что, если файл поврежден, его можно обнаружить полностью. Также возможно обнаружение ранее неизвестной вредоносной программы.

Однако у этого метода имеются недостатки. Файлы в системе обычно часто меняются, что приводит к увеличению числа случаев, когда обнаруживается, что они были повреждены обманным путем. Если вирус встроен в часто изменяющийся файл в системе, этот метод можно легко обойти. В этом случае обнаружение изменения в этом файле с помощью лог файла занимает много времени, что приводит к таким проблемам, как метод на основе сигнатур.

Обнаружение на основе аномалий. Метод, основанный на аномалиях, направлен на обнаружение необычных, вирусоподобных или потенциально вредных действий или особенностей. Эта идея также используется в системах IDS.

Фундаментальная проблема этого метода состоит в том, чтобы выяснить, какое состояние является нормальным, а какое нет, и определить разницу между этими двумя состояниями. Кроме того, существует проблема изменения нормального состояния и адаптации системы к этому состоянию. Это вызывает появление множества ложных сигналов. Достоинством этого метода является возможность обнаружения ранее неизвестной вредоносной программы.

Недостатки антивирусных программных средств. Антивирусное программное средство считается необходимым условием защиты компьютера. В общем, антивирус сканирует, защищает, помещает в карантин вредоносные программы и выполняет другие операции для компьютера. Антивирусное программное средство можно установить с CD-диска и через сеть Интернет. Антивирусные программные средства отличаются друг от друга множеством уникальных функций. Например, блокировка рекламы при использовании Интернета, блокировка проникновения вредоносных программ с Интернета и т.д. Однако пользователям не следует полностью полагаться на возможности антивирусных программных средств.

Антивирусные программные средства для непрерывного обнаружения вирусов нуждаются в образцовых файлах, которые

содержат самую свежую и обновленную информацию. Однако, до тех пор, пока производители антивирусов не создадут образцы файлов для нового вируса, создатели вирусов будут создавать все больше новых вирусов. Это означает, что подготовка вакцины от нового вируса требует много времени.

Кроме того, антивирусное программное обеспечение может оказаться бесполезным при обнаружении вредоносных программ типа Rootkit. Вредоносные программы типа Rootkit направлены на атаку центра операционной системы компьютера.

Факторы оценки качества антивирусного программного средства. Антивирусное программное средство можно оценить по следующим факторам:

- *надежность и удобства использования* – антивирусное программное средство не «зависает» и не требует различной подготовки к использованию;
- способность качественного обнаружения всех распространенных вирусов, сканирования файлов документов/ таблиц (MS Word, Excel), упакованных, архивных файлов и лечения зараженных объектов;
- доступность для всех популярных платформ (DOS, Windows NT, Novell NetWare, OS / 2, Alpha, Linux и др.), наличие режимов сканирования по запросу и быстрого сканирования;
- скорость обработки и другие особенности.

Профилактические меры. Своевременное обнаружение вирусов и зараженных файлов может предотвратить распространение вирусной эпидемии на другие компьютеры за счет полного устранения обнаруженных вирусов на каждом компьютере. Не существует абсолютно надежных программ, способных обнаружить и уничтожить любой вирус. Важный способ борьбы с компьютерными вирусами – своевременная профилактика. Чтобы значительно снизить вероятность заражения вирусом и обеспечить надежное хранение данных на дисках, необходимо принять следующие меры профилактики:

- использовать только лицензионное программное обеспечение;
- обеспечить компьютер современной антивирусной программой и регулярно обновлять ее;
- выполнять антивирусную проверку каждого накопителя перед чтением данных, записанных с другого компьютера;

- выполнять сканирование после распаковки файлов из архива;
- повторная проверка дисков компьютера на антивирусной программе;
- использование антивирусной программы для контроля всех исполняемых файлов, полученных из компьютерных сетей.

Антивирусные программные комплексы. У каждого антивирусного программного средства есть свои преимущества и недостатки. Комплексное использование всего нескольких антивирусных программных средств может обеспечить полную защиту. На практике существует множество антивирусных программных средств, в качестве примера можно привести следующие (табл. 7.3).

Таблица 7.3

Особенности различных антивирусных программ

Продукт / Свойства	McAfee AntiVirus Plus	Semantec Norton AntiVirus Plus	Kaspersky Anti-Virus	Bitdefender Antivirus Plus	Webroot SecureAnywhere Antivirus	Eset Nod32 Antivirus	Trend Micro Antivirus+ Security	F-secure Anti-Virus	VoodooSoft VoodooShield	The Kure
Стоимость	19.99$	19.99 $	29.99 $	29.99 $	18.99$	27.99$	29.95$	39.99$	19.99$	19.99$
Сканирование по спросу	+	+	+	+	+	+	+	+	-	-
Постоянное сканирование	+	+	+	+	+	+	+	+	+	-
Оценка веб сайта	+	+	+	-	+	-	+	-	-	-
Блокировка вредоносного URL	+	+	+	+	+	+	+	+	-	-
Защита от фишинга	+	+	+	+	+	+	+	-	-	-
Определение по признаку	+	+	+	+	+	+	+	+	+	-
Сканирование уязвимостей	+	-	+	+	-	-	-	-	-	-

Контрольные вопросы

1. Важность обеспечения безопасности в программных продуктах.
2. Причины возникновения проблем безопасности в программных продуктах.
3. Понятия дефект, баг, переполнение памяти.
4. Фундаментальные принципы безопасности программного средства.
5. Требования к программным средствам.
6. Требования к безопасности программных средств.
7. Роль языков программирования в безопасности программных средств.
8. Безопасные и небезопасные языки программирования.
9. Вредоносные программы и их основные типы.
10. Что такое компьютерные вирусы?
11. Методы и средства защиты от вредоносных программ.
12. Требования к выбору антивирусного программного средства.

ЛИТЕРАТУРА

1. Ганиев С.К., Кучкаров Т.А. Тармоқ хавфсизлиги (Мобил тармоқ хавфсизлиги):Ўқув қўлланма.Т.: Алоқачи, 2019. 140 б.
2. С.К. Ганиев, М.М. Каримов, З.Т. Худойқулов, М.М. Кадиров. Толкковый словарь терминов и понятий по безопасности информации на русском, узбекском и английском языках. Т.: Iqtisod-Moliya, 2017. 480 с.
3. Ганиев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Т.: Фан ва технология, 2016. 372 б.
4. Ганиев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги: Ўқув қўлланма. Т.: Алоқачи, 2008. 382 б.
5. Stamp M. Information security: principles and practice // John Wiley & Sons. 2011. P. 606.
6. А.С. Марков, А.В. Барабанов, А.В. Дорофеев, В.Л. Цирлов. Семь безопасных информационных технологий / Под ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
7. Д.Я. Акбаров, П.Ф. Хасанов, Х.П. Хасанов, О.П. Ахмедова, И.У. Холимтоева. Криптографиянинг математик асослари: Ўқув қўлланма. Т.:Алоқачи, 2019. 192 б.
8. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. Т., 2008. Б. 394.
9. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : Учебное пособие. М.: ИД ФОРУМ : ИНФРА-М, 2017. 416 с.
10. Raef Meeuwisse. Cybersecurity for Beginners (2nd. ed.). Cyber Simplicity Ltd. London, England, 2017. 224 p.
11. Manjikian M. Cybersecurity ethics: an introduction. Routledge, 2017. 328 p.
12. Kostopoulos G. Cyberspace and cybersecurity. CRC Press, 2017. 316 p.
13. Christen M., Gordijn B., Loi M. The Ethics of Cybersecurity. Springer Nature, 2020. С. 384.
14. Pande J. Introduction to Cyber Security. Uttarakhand Open University, 2017. 152 p.
15. Cybersecurity Fundamentals Study Guide, ISACA, 2015. 196 p.

16. Easttom C. Computer security fundamentals. Pearson IT Certification, 2019. 447 p.
17. Бондарев В.В. Введение в информационную безопасность автоматизированных систем: Учебное пособие. М. : МГТУ им. Н. Э. Баумана, 2016. 250 с.
18. Shinder D. L., Cross M. Scene of the Cybercrime. Elsevier, 2008.
19. K. Scarfone et al. Guide to storage encryption technologies for end user devices //NIST Special Publication. 2007. T. 800. C. 111.
20. Curricula Cybersecurity. Curriculum guidelines for post-secondary degree programs in cybersecurity. 2017.
21. Purdy G. ISO 31000: 2009-setting a new standard for risk management //Risk Analysis: An International Journal. 2010. T. 30. № 6. C. 881-886.
22. Zlatanov N. Hard Disk Drive and Disk Encryption, 2015. DOI: 10.13140/RG.2.1.1228.9681.
23. Ganiev S.K., Khudoykulov Z.T., Islomov Sh.Z. Selection suitable biometrics for cryptographic key generators // TUIT BULLETIN. T., 2016. №4 (40). P. 80-92
24. Rathgeb C., Uhl A. A survey on biometric cryptosystems and cancelable biometrics //EURASIP Journal on Information Security. 2011. №1. P. 1-25.
25. Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2015, 2016, and 2017. U.S. Department of Health and Human Services Office for Civil Rights. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2015-2016-2017.pdf

Интернет ресурсы

1. ACR39U smart card rader [сайт]: http://smartkardtechnologies.com/productdetails/acr39u-smart-card-rader (время обращения: 29.10.2020).
2. Certified Network Defender [сатйт]: https://iclass.eccouncil.org/our-courses/certified-network-defender-cnd/ (время обращения: 29.10.2020).
3. 3D Airport Security X-ray Machine [сайт]: https://www.turbosquid.com/3d-models/3d-airport-x-ray-machine-security-1405223 (время обращения: 29.10.2020).

4. Web Applications vulnerabilities and threats: statistics for 2019 [сайт]: https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/ (время обращения: 29.10.2020).
5. How to Spot Phishing Emails [сайт]: https://www.nuigalway.ie/itsecurity/howtospotphishingemails/ (время обращения: 29.10.2020).
6. Beware of fake microsoft security essentials [сайт]: https://techjaws.com/beware-of-fake-microsoft-security-essentials/ (время обращения: 29.10.2020).
7. The Best Antivirus Protection for 2020 [сайт]: https://www.pcmag.com/roundup/256703/the-best-antivirus-protection (время обращения: 29.10.2020).
8. Securing Wireless Networks [сайт]: https://www.us-cert.gov/ncas/tips/ST05-003 (время обращения: 29.10.2020).
9. Why High Availability Is Important for Your Business [сайт]: https://blog.layershift.com/why-high-availability-for-your-business/ (время обращения: 29.10.2020).
10. Рутокен [сайт]: https://www.rutoken.ru/ (время обращения: 29.10.2020).
11. Comparison of disk encryption software [сайт]: https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software (время обращения: 29.10.2020).
12. G20 summit: NSA targeted Russian president Medvedev in London [сайт]: https://www.theguardian.com/world/2013/jun/16/nsa-dmitry-medvedev-g20-summit (время обращения: 29.10.2020).
13. CRADC Data Destruction and Return of Restricted Data Policy [сайт]: https://ciser.cornell.edu/wp-content/uploads/2017/01/CRADC_Destruction_and_Return_of_Restricted_Data.pdf (время обращения: 29.10.2020).
14. Privacy Impact Assessment Integrated Automated Fingerprint Identification System National Security Enhancements [сайт]: https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis (время обращения: 29.10.2020).
15. Best Keylogger for Windows 10 in 2020 [сайт]: https://www.pctattletale.com/blog/1505/best-keylogger-software-windows-10 (время обращения: 29.10.2020).
16. Windows Event Logging and Forwarding [сайт]: https://www.cyber.gov.au/acsc/view-all-content/publications/windows-event-logging-and-forwarding (время обращения: 29.10.2020).

СПИСОК СОКРАЩЕНИЙ

ABAC – Attribute-based access control

AES – Advanced Encryption Standard

APT – Advanced persistent threats

ASCII – American Standard Code for Information Interchange

ИТ – Информационные технологии

CBC – Cipher Block Chaining

CCTV – Closed-circuit television

CDMA – Code Division Multiple Access

CSEC2017 JTF – Cybersecurity Curricula 2017 Joint Task Force

CVE – Common Vulnerabilities and Exposures

DAC – Discretionary access control

DES – Data Encryption Standard

DLP – Data Leakage Prevention

DoD – Department of Defense

DoS – Denial of service

ECB – Electronic codebook mode

FAR – False Acceptance Rate

FRR – False Rejection Rate

FTP – File Transfer Protocol

GNFS – General Number Field Sieve

GSM – Global System for Mobile Communications

HMAC – Hash-based message authentication code

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

IDS – Instrusion Detection System

IPS – Intrusion Prevention System

IPSec – IP Security

ISO – International Organization for Standardization

IV – Initialization Vector

KDC – Key Destribution Center

L2TP – Layer 2 Tunneling Protocol

LAN – Local Area Network

MAC – Mandatory access control

MAC – Message Authentication Code

MAN – Metropolitan Area Network

MITM – Man in the middle attack

NAT – Network Address Translation

OWASP – Open Web Application Security Project

PAN – Personal Area Network

PIN – Personal Identification Number

PKI – Public key infrastructure

PPP – Point-to-Point Protocol

PPTP – Point-to-Point Tunneling Protocol

RAID – Redundant Array of Independent Disks

RBAC – Role-based access control

RFID – Radio Frequency IDentification

SIM – Security Information Management

SSID – Service Set Identifier

SSL – Secure Sockets Layer

TCP/IP – Transmission Control Protocol/Internet Protocol

USB – Universal Serial Bus

UTM – Unifield Threat Management

VPN – Virtual Private Network

WAN – Wide Area Network

WEP – Wired Equivalent Privacy

WLAN – Wireless Local Area Network

WMAN – Wireless Metropolitan Area Network

WPA – Wi-Fi Protected Access

WPAN – Wireless Personal Area Network

WWAN – Wireless Wide Area Network

ОБА – Онлайн банк Алисы

ATM – Automated teller machine

MAC – Media access control

ОС – Операционная система

ЭЦП– Электронная цифровая подпись

ГЛОССАРИЙ

Авторизация – представление пользователю определенных прав доступа на основе положительного результата его аутентификации в системе.
Avtorizatsiya – tizimda foydalanuvchiga, uning ijobiy autentifikatsiyasiga asosan, ma’lum foydalanish huquqlarini taqdim etish.
Authorization – granting the user certain access rights based on the positive result of authentication in the system.

Администратор защиты – субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.
Himoya ma’muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz foydalanishdan himoyalashga javobgar foydalanish subyekti.
Security administrator – the subject of the access responsible for the protection of the automated system against unauthorized access to the information.

Администратор системы – лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии.
Tizim ma’muri – tizimni ekspluatatsiyasiga va uning ishga layoqatlik holatini ta’minlashga javobgar shaxs.
System administrator – a person who is responsible for operation of the system and keeping it in an appropriate working condition.

Актив – 1. Информация или ресурсы, подлежащие защите. 2. Все, что имеет ценность для организации. 3. Главное приложение, общая система поддержки, высоко авторитетная программа, материальная часть, миссия критической системы, персонал, оборудование или логически связанная группа систем.
Aktiv – 1. Himoyalanuvchi axborot yoki resurslar. 2. Tashkilot uchun qiymatli barcha narsalar. 3. Bosh ilova, umumiy madadlovchi tizim, yuqori nufuzli dastur, moddiy qism, kritik tizim missiyasi, xodimlar, jihozlar yoki mantiqiy bog’langan tizimlari guruhi.
Asset – 1. Information or resources that should be protected. 2. Anything that has value to the organization. 3. A major application, general support system, high impact program, physical plant, mission

critical system, personnel, equipment, or a logically related group of systems.

Активная угроза – угроза преднамеренного несанкционированного изменения состояния системы.
Faol tahdid – tizim holatini atayin ruxsatsiz o’zgartirish tahdidi.
Active threat – a threat that can make a deliberate unauthorized change to the system.

Алгоритм шифрования – алгоритм криптографический, реализующий функцию шифрования. В случае блочных шифрсистем получается с использованием алгоритма шифрования блочного базового в конкретном режиме шифрования.
Shifrlash algoritmi – shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm. Blokli shifrtizim holida shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.
Encryption algorithm – a cryptographic algorithm that implements the function of encryption. In the case of block cipher system is obtained using the algorithm of the base block encryption in a particular mode of encryption.

Алгоритм криптографический – алгоритм, реализующий вычисление одной из криптографических функций.
Kriptografik algoritm – kriptografik funksiyalardan birini hisoblashni amalga oshiruvchi algoritm.
Cryptographic algorithm – the algorithm that implements the calculation of one cryptographic functions.

Алгоритм расшифрования – алгоритм криптографический, обратный к алгоритму шифрования и реализующий функцию расшифрования.
Deshifrlash algoritmi – deshifrlash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritm.
Decryption algorithm – the cryptographic algorithm which is inverse to the encryption algorithm that implements the decryption function.

Алгоритм хеширования – в криптографии - алгоритм, реализующий хеш-функцию криптографическую. В математике и

программировании - алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале - от всех). Обычно, алгоритм хеширования преобразует строки произвольной длины в строки фиксированной длины.

Xeshlash algoritmi – kriptografiyada kriptografik xesh-funksiyani amalga oshiruvchi algoritm. Matematika va dasturlashda – odatda, satr uzunligini kamaytiruvchi simvollar satrini o'zgartiruvchi algoritm. Chiqish yo'li satrining har bir simvolining qiymati kirish yo'li simvollarining katta soniga (idealda – barchasiga) murakkab tarzda bog'liq. Odatda xeshlash algoritmi ixtiyoriy uzunlikdagi satrni belgilangan uzunlikdagi satrga o'zgartiradi.

Hashing algorithm – in cryptography, an algorithm that implements the cryptographic hash function. In mathematics and computer programming - algorithm for converting strings of characters, generally reducing the length of the string and such that the value of each symbol of the output string depends in a complex way from a large number of input characters (ideally all). Usually, hashing algorithm converts strings of arbitrary length to strings of fixed length.

Алгоритм цифровой подписи – асимметричный алгоритм, используемый для цифровой подписи данных.

Raqamli imzo algoritmi – ma'lumotlarni raqamli imzolash uchun foydalaniluvchi asimetrik algoritm.

Digital signature algorithm – asymmetric algorithm used for digitally signing data.

Алгоритм шифрования RSA – алгоритм шифрования, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом, и предназначенный для построения шифрсистем асимметричных.

RSA shifrlash algoritmi – 1978 yili R. Rayvest, A Shamir va L.Adleman tomonidan taklif etilgan va asimetrik shifr tizimlarini qurishga mo'ljallangan shifrlash algoritmi.

RSA encryption algorithm – the encryption algorithm proposed in 1978 by R. Rivest, A. Shamir and L. Adleman and is designed to build asymmetric ciphers.

Анализ – изучение значимости полученных данных и доказательственной ценности к случаю.
Tahlil – olingan ma’lumotlarning muhimligi va vaziyat uchun isbotlanganlik qiymatini o’rganish.
Analysis – the examination of acquired data for its significance and probative value to the case.

Анализаторы сетевые (сниффер) – программы, осуществляющие «прослушивание» трафика сетевого и автоматическое выделение из трафика сетевого имен пользователей, паролей, номеров кредитных карт, другой подобной информации.
Tarmoq tahlillagichlari (sniffer) – tarmoq trafigini “tinglash”ni va tarmoq trafigidan avtomatik tarzda foydalanuvchilar ismini, parollarni, kredit kartalar nomerini, shu kabi boshqa axborotni ajratib olishni amalga oshiruvchi dasturlar.
Network analyzers (sniffer) – programs that listen on network traffic and automatic allocation of network traffic usernames, passwords, credit card numbers, and other such information.

Антивирус – программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Если вирус удалить не удается, то зараженная программа уничтожается. Еще – программа, предназначенная для защиты от вирусов, обнаружения зараженных программных модулей и системных областей, а также восстановления исходного состояния зараженных объектов.
Antivirus – viruslarni aniqlovchi yoki aniqlovchi va yo’q qiluvchi dastur. Agar virus yo’q qilinmasa, zaharlangan dastur yo’q qilinadi. Yana – viruslardan himoyalashga, zaxarlangan dasturiy modullar va tizimli makonlarni aniqlashga, hamda zaxarlangan obyektlarning dastlabki holatini tiklashga mo’ljallangan dastur.
Antivirus – the program that detect or detect and remove viruses. If virus remove not possible, then the infected program is destroyed. Another program, designed to protect against viruses, detecting infected software modules and system areas as well as restore the original state of infected object.

Аппаратное средство защиты информации – специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.
Axborotni himoyalashning apparat vositasi – axborotni ishlovchi texnik vositasi komplekti tarkibiga kiruvchi maxsus himoyalovchi qurilma yoki moslama.
Hardware data protection – a special protective device or fixture included in the kit technical tools of information processing.

Апплеты вредоносные – небольшие приложения, которые автоматически загружаются и выполняются, и которые реализуют несанкционированные функции информационной системы.
Zararli appletlar – axborot tizimida ruxsat etilmagan funksiyalarni amalga oshiruvchi, avtomatik yuklanuvchi va bajariluvchi kichik ilovalar.
Malicious applets – small application that are automatically downloaded and executed and that perform an unauthorized function on an information system.

Архитектура IT безопасности – описание принципов безопасности и общего подхода для соблюдения принципов, управляющих системой проектирования безопасности.
AT xavfsizlik arxitekturasi – xavfsizlikni loyihalash tizimini boshqaruvchi prinsiplariga rioya qilish uchun xavfsizlik prinsiplarining va umumiy yondashishning tavsifi.
IT security architecture – a description of security principles and an overall approach for complying with the principles that drive the system design.

Архитектура информационной безопасности – встроенная, неотъемлемая часть архитектуры предприятия, описывающая структуру и поведение процессов безопасности, систем информационной безопасности, персональных и организационных подразделений, с указанием их выравнивание с целью и стратегическими планами предприятия.
Axborot xavfsizligining arxitekturasi – tashkilot xavfsizlik jarayonlari strukturasi va ishlash rejimini, axborot xavfsizligi tizimlarini, shaxsiy va tashkiliy bo’linmalarini, ularni tashkilot missiyasi va strategik rejalariga

tenglashtirishni ko’rsatish bilan tavsiflovchi tashkilot arxitekturasining o’rnatilgan, ajratib bo’lmas qismi.

Information security architecture – an embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise’s security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise’s mission and strategic plans.

Атака «противник в середине» – атака на протокол криптографический, в которой противник С выполняет этот протокол как с участником А, так и с участником В. Противник С выполняет сеанс с участником А от имени В, а с участником В от имени А. В процессе выполнения противник пересылает сообщения от А к В и обратно, возможно, подменяя их. В частности, в случае протокола аутентификации абонента успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для В под именем А. Для осуществления атаки «противник в середине» необходимо обеспечивать синхронизацию двух сеансов протокола.

«Dushman o’rtada» xujumi – kriptografik protokolga hujum bo’lib, bunda dushman C ushbu protokolni ishtirokchi A va ishtirokchi B bilan bajaradi. Dushman C ishtirokchi A bilan seansni ishtirokchi B nomidan, ishtirokchi B bilan esa ishtirokchi A nomidan bajaradi. Bajarish jarayonida dushman ishtirokchi A dan ishtirokchi V ga va aksincha xabarni, ehtimol, o’zgartirib uzatadi. Xususan, abonentni autentifikatsiyalash protokoli holida «dushman o’rtada» hujumining muvafaaqiyatli amalga oshirilishi dushmanga ishtirokchi B uchun o’zini ishtirokchi A nomidan autentifikatsiyalashga imkon beradi. «Dushman o’rtada» hujumini amalga oshirish uchun protokolning ikkita seansining sinxronlanishini ta’minlash lozim.

Attack “the opponent in the middle” – attack on a cryptographic protocol in which the enemy with this protocol performs as a party A and party B with C. Enemy performs session with party A on behalf of B, and a participant on behalf of A. During runtime opponent forwards messages from A to B and back, possibly replacing them attacks. In particular, in the case of an authentication protocol is connected to the success of the attack “the opponent in the middle” allows authenticate itself to the enemy in the name of A. To carry out the attack “the

opponent in the middle" is necessary to ensure the synchronization of the two sessions of the protocol.

Атака на отказ в обслуживании – атака с целью вызвать отказ системы, то есть создать такие условия, при которых легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет значительно затруднён.
Xizmat qilishdan voz kechishga undaydigan hujum – tizim buzilishiga sabab bo'luvchi hujum, ya'ni shunday sharoitlar tug'diradiki, qonuniy foydalanuvchi tizim taqdim etgan resurslardan foydalana olmaydi yoki foydalanish anchagina qiyinlashadi.
Denial-of-service attack – attack intended to cause a system failure, that is, to create conditions under which legitimate users will not be able to access the system-provided resources, or this access much more difficult.

Атака пассивная – атака на криптосистему или протокол криптографический, при которой противник и/или нарушитель наблюдает и использует передаваемые сообщения шифрованные, но не влияет на действия пользователей законных.
Passiv hujum – kriptotizmga yoki kriptografik protokolga hujum bo'lib, bunda dushman va/yoki buzg'unchi uzatiluvchi shifrlangan axborotni kuzatadi va ishlatadi, ammo qonuniy foydalanuvchilar harakatiga ta'sir etmaydi.
Passive attack – attack on a cryptosystem or a cryptographic protocol in which enemy and/or the offender observes and uses the transmitted messages are encrypted, but does not affect the user's actions legitimate.

Атака со словарем паролей – атака на криптосистему, основанная на переборе значений пароля.
Parollar lug'atiga asoslangan hujum – parol qiymatlarini saralashga asoslangan kriptotizimga hujum.
Attack with a dictionary of passwords – the attack on the cryptosystem based on iterating the value of a password.

Аутентификатор – средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова,

биометрические данные и другие отличительные признаки пользователя.

Autentifikator – foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo'shimcha kod so'zlari, biometrik ma'lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo'lishi mumkin.

Authenticator – means of authentication that represents the distinctive attribute of the user. Means of user authentication can be additional code word, biometric data and other identifying features of the user.

Аутентификация – проверка идентификации пользователя, устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.

Autentifikatsiya – odatda tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul uchun foydalanuvchining, qurilmaning yoki tizimning boshqa tashkil etuvchisining identifikasiyasini tekshirish; saqlanuvchi va uzatuvchi ma'lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.

Authentication – checking the identification of user, device, or other component in the system, typically for decision-making about access to system resources; check the integrity of stored or transmitted data to detect unauthorized modification.

Аутентификация биометрическая – способ аутентификации абонента (пользователя), основанный на проверке его биометрических характеристик (отпечатков пальцев, геометрии руки, лица, голоса, рисунка сетчатки глаза и т.п.). К преимуществам данного метода относится неотделимость биометрических характеристик от пользователя: их нельзя забыть, потерять или передать другому пользователю.

Biometrik autentifikatsiya – abonentni (foydalanuvchini) uning biometrik xarakteristikasi (barmoq izlari, panja geometriyasi, yuzi, ovozi, ko'z pardasining to'ri va h.) asosidagi autentifikatsiyalash usuli. Ushbu usulning afzalligi – biometrik xarakteristikalarni foydalanuvchidan ajratib bo'lmasligi. Ularni esdan chiqarishning, yo'qotishning yoki boshqa foydalanuvchiga berishning iloji yo'q.

Biometric authentication – the method of authentication of a subscriber (user), based on a verification of biometric characteristics (fingerprints, hand geometry, face, voice, eye retina image, etc.). The advantages of this method is the inseparability of biometric characteristics from user: they cannot be forgotten, lost or transferred to another user.

Аутентификация двухфакторная – аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).
Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.
Two-factor authentication – user authentication on the basis of two unrelated factors, as a rule, on the basis of what he knows and what he knows (e.g., password-based and physical ID).

Аутентификация на основе паролей одноразовых – технология аутентификации с помощью паролей одноразовых, для получения которых могут использоваться: алгоритм генерации на основе односторонней функции, специальные устройства – токены, либо технология OOB (out of band), основанная на передаче пароля одноразового с использованием дополнительного канала, отличного от того, по которому пользователь осуществляет доступ к прикладной системе.
Bir martali parollar aosidagi autentifikatsiya – bir martali parollar yordamida autentifikatsiyalash texnologiyasi. Bir martali parollarni olishda quydagilar ishlatilishi mumkin: bir tomonlama funksiya asosida generatsiyalash algoritmi, maxsus qurilmalar-tokenlar, yoki bir martali parolni, foydalanuvchi tatbiqiy tizimdan foydalanishda ishlatiladigan kanaldan farqli, kanal orqali uzatishga asoslangan OOB (out of band) texnologiyasi.
One time password based authentication – technology authentication using one time passwords, which can be used: the generation algorithm based on one-way functions, special device – taken, or technology OOB (out of band) based on the transmission password disposable using additional channels, other than where the user accesses the application system.

Аутентификация сообщений – добавление к блоку данных контрольного поля для обнаружения любых изменений в данных. При вычислении значений этого поля используется ключ, известный только приемнику данных.
Xabarlar autentifikatsiyasi – ma’lumotlarda har qanday o’zgarishlarni aniqlash maqsadida ma’lumotlar blokiga nazorat hoshiyasini qo’shish. Ushbu hoshiya qiymatini hisoblashda faqat ma’lumotlar priyemnigiga ma’lum kalitlar ishlatiladi.
Message authentication – adding control data to the data field to detect any changes in the data. The values of this field using a key known only to receiver data.

База данных – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ. Является информационной моделью предметной области. База данных, как правило, представляется тремя уровнями абстракции: внешним, концептуальным и внутренним.
Ma’lumotlar bazasi – tatbiqiy dasturlarga bog’liq bo’lmagan holda ma’lumotlarni tavsiflashning, saqlashning va manipulyatsiyalashning umumiy prinsiplarini ko’zda tutuvchi, ma’lum qoidalar bo’yicha tashkil etilgan ma’lumotlar majmui. Predmet sohasining informatsion modeli hisoblanadi. Ma’lumotlar bazasi odatda abstraksiyaning tashqi, konseptual va ichki satxlari orqali ifodalanadi.
Database – a collection of data organized according to certain rules, providing general principles for describing, storing and manipulating data independent of the application programs. An information domain model. The database, usually presented in three levels of abstraction: external, conceptual and internal.

Безопасность – свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. Еще – состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами.

Xavfsizlik – ta’siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifiy, ichki va tashqi beqarorlovchi faktorlarga qarshi tizimning tura olish xususiyati. Yana - ma’lumotlar fayllarining va dasturlarning avtorizatsiyalanmagan shaxslar (jumladan tizim xodimi), kompyuterlar yoki dasturlar tomonidan ishlatilishi, ko’rib chiqilishi va modifikatsiyalanishi mumkin bo’lmagan holat.
Security – the property of a system to withstand external or internal destabilizing factors, the effect of which may be unwanted state or behaviour. Still - a state in which the data files and programs may not be used, viewed and modified by unauthorized persons (including the system staff), computers or software.

Безопасность информации – состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение; еще – состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность (конфиденциальность), целостность и доступность.
Axborot xavfsizligi – axborot holati bo’lib, unga binoan axborotga tasodifiy yoki atayin ruxsatsiz ta’sir etishga yoki ruxsatsiz uning olinishiga yo’l qo’yilmaydi; yana - axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanish darajasi holati.
Information security – status information, which excludes accidental or deliberate tampering or unauthorized information receive it, also - the state of security level information when processing technical means to ensure the preservation of its quality characteristics (properties) such as secrecy (confidentiality), integrity, and availability.

Безопасность информационная общества – то же, что и «безопасность, информационная личности» применительно к организованному коллективу людей и к обществу в целом.
Jamiyat axborot xavfsizligi – “shaxs axborot xavfsizligi” kabi, uyushgan odamlar kollektiviga va umuman, jamiyatga qo’llaniladi.
Society information security – what “safety information personality” when applied to organized team of people and to society as a whole.

Безопасность информационной сети – меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.
Axborot tarmog'i xavfsizligi – axborot tarmog'ini ruxsatsiz foydalanishdan, me'yoriy harakatlariga tasodifiy yoki atayin aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.
Network security – measures that protect the information network from unauthorized access, accidental or deliberate interference in normal activities or attempts the destruction of its components.

Брандмауэр – метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами; еще – является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра).
Tarmoqlararo ekran – apparat-dasturiy vositalar yordamida tarmoqdan foydalanishni markazlashtirish va uni nazoratlash yo'li bilan tarmoqni boshqa tizimlardan va tarmoqlardan keladigan xavfsizlikka tahdidlardan himoyalash usuli; yana - bir necha komponentlardan (masalan, tarmoqlararo ekran dasturiy ta'minoti ishlaydigan marshrutizator yoki shlyuzdan) tashkil topgan ximoya to'sig'i hisoblanadi.
Firewall – a method of protecting a network against security threats from other systems and networks, through centralizing network access and control hardware and software; - is a protective barrier consisting of several components (e.g., router or gateway running firewall software).

Кибер инфраструктура – включает электронную информацию и коммуникационные системы, и службы и информацию, содержавшуюся в этих системах и службах.
Kiber infrastruktura – elektron axborot, kommunikatsiya tizimlari, xizmatlar va bu tizimlar va xizmatlarda mavjud axborotni o'z ichiga oladi.
Cyber infrastructure – includes electronic information and communications systems and services and the information contained in these systems and services.

Кибер инцидент – действия, использующие компьютерные сети, приводящие к фактическому или потенциальному ущербу в информационной системе и/или содержащейся в ней информации.
Kiber insident – axborot tizimi va/yoki undagi axborotga aniq yoki potensial zarar yetkazilishiga sabab bo'luvchi, kompyuter tarmoqlaridan foydalanuvchi harakatlar.
Cyber incident – actions taken using computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

Кибер-атака – атака, через киберпространство, предназначенная для использования предприятием киберпространства в целях, отключения, уничтожения или злонамеренного контроля вычислительной среды/инфраструктуры**.**
Kiber-hujum – hisoblash muhiti/ infrastrukturasini, o'chirish, buzish yoki g'arazli nazoratlash yoki ma'lumot yaxlitligini buzish yoki nazoratlanuvchi axborotni o'g'irlash maqsadida kiberfazodan foydalanuvchi tashkilotga atalgan kiberfazo orqali amalga oshiriluvchi hujum.
Cyber-attack – an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disabling, destroying, or maliciously controlling a computing environment/infrastructure.

Кибербезопасность – возможность охранять или защитить использование киберпространства кибератаками.
Kiberxavfsizlik – kiberfazoning kiberhujumlardan foydalanishidan qo'riqlash yoki himoyalash imkoniyati.
Cybersecurity – the ability to protect or defend the use of cyberspace from cyber-attacks.

Киберпреступность – действия отдельных лиц или групп, направленные на взлом систем компьютерной защиты, на хищение или разрушение информации в корыстных или хулиганских целях.
Kiberjinoyatchilik – g'arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o'g'irlashga yoki buzishga yo'naltirilgan alohida shaxslarning yoki guruhlarning harakatlari.

Cyber cryme – the actions of individuals or groups aimed at cracking computer security systems, theft or destruction of information for selfish or destructive purposes.

Киберпространство – глобальный домен в информационной среде, состоящий из взаимозависимой сети инфраструктур информационных систем включая Интернет, сети телекоммуникации, компьютерные системы, и встроенные процессоры и контроллеры.
Kiberfazo – Internet, telekommunikatsiya tarmoqlari, kompyuter tizimlari va o'rnatilgan prosessorlar va kontrollerlarni o'z ichiga olgan, o'zaro bog'langan axborot tizimlari infrastrukturalar tarmog'idan tashkil topgan axborot muhitidagi global domen.
Cyberspace – a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Кибертерроризм – действия по дезорганизации компьютерных систем, создающие опасность гибели людей, значительного имущественного ущерба либо иных общественно опасных последствий.
Kiberterrorizm – insonlar halokati, aytarlicha moddiy zarar xavfini yoki boshqa jamiyatga xavfli oqibatlarni tug'diruvchi kompyuter tizimlarini izdan chiqarish bo'yicha harakatlar.
Cyber terrorism – action disruption of computer systems, creating a danger of loss of life, significant property damage or other socially dangerous consequences.

Привилегии – права пользователя или программы, состоящие в доступности определенных объектов и действий в вычислительной системе.
Imtiyozlar – hisoblash tizimida ma'lum obyektlardan foydalanish va ularda ishlashdan iborat foydalanuvchilarning yoki dasturning huquqlari.
Privilege – rights of the user or a program, consisting in the availability of certain objects and actions in a computing system.

Приложение – программное обеспечение (программа) информационной системы, выполняющая определенную функцию

непосредственно для пользователя без доступа к системе управления, мониторинга или административным привилегиям.
Ilova – bevosita foydalanuvchi uchun boshqarish, monitoringlash tizimlaridan yoki ma’muriy imtiyozlardan foydalanmay aniq funksiyani bajaruvchi axborot tizimining dasturiy ta’minoti (dasturi).
Application – a software (program) hosted by an information system. In addition, software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

Программа антивирусная – программа компьютерная, предназначенная для защиты от вирусов компьютерных. Осуществляет обнаружение, восстановление, блокирование и/или удаление зараженных программных модулей и системных областей.
Virusga qarshi dastur – kompyuter viruslaridan himoyalashga mo’ljallangan kompyuter dasturi. Zaharlangan dasturiy modullarni va tizim sohalarini aniqlashni, tiklashni, blokirovka qilishni va/yoki yo’q qilishni amalga oshiradi.
Antivirus program – a computer program designed to protect the viruses from the computer. Detection, recovery, blocking and/or deleting infected software modules and system areas.

Виртуальная частная сеть – виртуальная сеть, построенная на основе существующих физических сетей, обеспечивающая безопасный туннель коммуникации для передачи данных или другой информации, передаваемой между сетями.
Virtual shaxsiy tarmoq – tarmoqlar orasida almashiniluvchi ma’lumotlar yoki boshqa axborotni uzatish uchun xavfsiz kommunikatsiya tunnelini ta’minlovchi, mavjud fizik tarmoqlar asosida qurilgan virtual tarmoq.
Virtual private network – a virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

Контроль доступа на основе ролей – модель для управления доступом к ресурсам, когда разрешенные действия на ресурсы

идентифицированы с ролями, а не с личными идентификаторами субъекта.

Rollarga asoslangan ruxsatni nazoratlash – resurslardan foydalanishni boshqarish modeli bo'lib, resurslarda ruxsat berilgan harakatlar shaxsiy subyekt identifikatorining o'rniga rollar bilan identifikatsiyalanadi.

Role-based access control – a model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

Конфиденциальность – 1. Некоторый класс данных, получение либо использование которых неавторизованными для этого лица не может стать причиной серьезного ущерба для организации. 2. Свойство информации, состоящее в том, что она не может быть обнаружена и сделана доступной без разрешения отдельным лицам, модулям или процессам.

Konfidensiallik – 1. Avtorizatsiyalanmagan shaxs tomonidan olinishi yoki foydalanishi tashkilot uchun jiddiy zarar sababi bo'la olmaydigan ma'lumotlarning qandaydir sinfi. 2. Alohida shaxslar, modullar, jarayonlar ruxsatisiz aniqlanishi, va foydalanishi mumkin bo'lmagan axborot xususiyati.

Confidentiality – 1. Some class data, obtaining or the use of which by unauthorized persons could not cause serious damage to the organization. 2. The quality of information, consisting in that it cannot be detected and made available without the permission of individuals, modules or processes.

Менеджмент риска – полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий.

Risk menejmenti – axborot-telekommunikatsiya texnologiya resurslariga ta'sir etishi mumkin bo'lgan xavfli xodisalar oqibatlarini identifikatsiyalashning, nazoratlashning, bartaraf etishning yoki kamaytirishning to'liq jarayoni.

Risk management – the complete process of identification, control, eliminate or mitigate the consequences of hazardous events that may affect resources of information and telecommunication technologies.

Целостность – свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому физическому её состоянию).
Yaxlitlik – axborotning buzilmagan ko’rinishda (axborotning qandaydir fizik holatiga nisbatan o’zgarmagan shaklda) mavjud bo’lishida ifodalangan xususiyati.
Integrity – the property of information, namely, its existence in an undistorted view (unchanged with respect to some physical condition).

ОГЛАВЛЕНИЕ

ДЛЯ ЗАМЕТОК

С.К. ГАНИЕВ, З.Т. ХУДОЙКУЛОВ, Н.Б. НАСРУЛЛАЕВ

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Учебное пособие

Редактор **Э. Хуснутдинова**
Художник **К. Бойхужаев**
Компьютерная верстка **К. Бойхужаев**

Лиц. изд. AI № 305. Подписано в печать 23.04.2021.
Формат 60x84 1/16. Усл.печ. л. 13,8.
Уч.-изд. л. 14,4. Тираж 50 экз.
Заказ № 29.

Издательство «IQTISOD-MOLIYA».
100000, Ташкент, ул. Амира Темура, 60^{A}.

Отпечатано в типографии
«DAVR MATBUOT SAVDO» ООО.
100198, Ташкент, Куйлюк, массив 4, 46.