ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
КЫРГЫЗСКО-РОСИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ АРХИТЕКТУРЫ, ДИЗАЙНА И СТРОИТЕЛЬСТВА

Кафедра «Защита в чрезвычайных ситуациях КРСУ и МЧС КР»

НЕКОТОРЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ЧАСТЬ III
ПРОГРАММНО-ТЕХНИЧЕСКИЕ СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. СУБД.

Учебно-методическое пособие

Бишкек 2019

УДК 004
Н 47

Рецензенты:
Г.И. Логинов, д-р техн. наук, профессор,
М.Д. Назарбеков, нач. службы спасения УМЧС КР по г. Бишкек

Составители:
А. Акбай кызы, Б.С. Ордобаев, Э. Эргешов

Рекомендовано к изданию кафедрой
«Защита в чрезвычайных ситуациях КРСУ и МЧС КР»

Н 47 НЕКОТОРЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Часть III. Программно-технические способы и средства обеспечения информационной безопасности. СУБД: учебно-методическое пособие / сост.: А. Акбай кызы, Б.С. Ордобаев, Э. Эргешов. – Бишкек: Изд-во КРСУ, 2019. – 106 с.

Изложены основные составляющие информационной безопасности, дополнена информация о понятии информации и информационной безопасности, о которой мы писали в первой части данного учебно-методического пособия, объекты ее защиты и программно-технические способы и средства обеспечения информационной безопасности, также раскрыты исторические аспекты возникновения и развития информационной безопасности, в том числе и криптография. Была затронута система управления базами данных, где широко раскрыто само определение базы данных, в том числе их история и настройка разрешений для базы данных Access.

Предназначено для студентов направления «Техносферная безопасность», а также инженерно-технических работников, интересующихся вопросами информационной безопасности.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В практике информационными технологиями обучения называют все технологии, использующие специальные технические информационные средства (ЭВМ, аудио, кино, видео).

Когда компьютеры стали широко использоваться в образовании, появился термин «новая информационная технология обучения».

Компьютерные технологии развивают идеи программированного обучения, открывают совершенно новые, еще не исследованные технологические варианты обучения, связанные с уникальными возможностями современных компьютеров и телекоммуникаций. Компьютерные (новые информационные) технологии обучения – это процессы подготовки и передачи информации обучаемому, средством осуществления которых является компьютер.

Использование информационных технологий повышает эффективность урока, развивая мотивацию обучения, что делает процесс обучения более успешным.

Информационные технологии не только открывают возможности вариативности учебной деятельности, ее индивидуализации и дифференциации, но и позволяют по-новому организовать взаимодействие всех субъектов обучения, построить образовательную систему, в которой обучающийся был бы активным и равноправным участником образовательной деятельности.

Информационные технологии значительно расширяют возможности предъявления учебной информации, вовлекают обучающихся в учебный процесс, способствуя наиболее широкому раскрытию их способностей, активизации умственной деятельности.

Процессы информатизации современного общества и тесно связанные с ними процессы информатизации всех форм образовательной деятельности характеризуются процессами совершенствования и массового распространения современных информационных и коммуникационных технологий. Подобные технологии активно применяются для передачи информации

и обеспечения взаимодействия преподавателя и обучаемого в современных системах открытого и дистанционного образования. Современный преподаватель должен не только обладать знаниями в области ИКТ, но и быть специалистом по их применению в своей профессиональной деятельности, не говоря уже о студентах, стремительно шагающих в ногу с новыми инновациями, связанными именно с компьютерными технологиями.

Слово *«технология»* имеет греческие корни и в переводе означает науку, совокупность методов и приемов обработки или переработки сырья, материалов, полуфабрикатов, изделий и преобразования их в предметы потребления. Современное понимание этого слова включает и применение научных и инженерных знаний для решения практических задач. В таком случае информационными и телекоммуникационными технологиями можно считать технологии, направленные на обработку и преобразование информации.

Информационные и коммуникационные технологии (ИКТ) – это обобщающее понятие, описывающее различные устройства, механизмы, способы, алгоритмы обработки информации. Важнейшим современным устройствами ИКТ являются компьютер, снабженный соответствующим программным обеспечением и средства телекоммуникаций вместе с размещенной на них информацией.

Соответственно, с развитием информационных технологий развивается и опасность информации, где мы искали объяснения информационной безопасности и описывали наиболее важнейшие факторы для обучения информационной безопасности.

СОКРАЩЕНИЯ, ИСПОЛЬЗУЕМЫЕ В ТЕКСТЕ

СМИБ – Система менеджмента информационной безопасности
ИТ – информационные технологии
ЛЭП – линии электропередач
ISDN – цифровая сеть интеграцией служб
TDM – мультиплексирование по времени
xDSL – цифровая абонентская линия
ATM – асинхронный способ передачи данных
ПК – персональный компьютер
ИКТ – информационно-коммуникационных технологий
НТР – научно-практическая революция
FTP – протокол передачи файлов по сети
ИС – информационные системы
БС – базовые станции
АОВС – аппаратное обеспечение вычислительных систем
ПУ – периферийное устройство
СУБД – система управления базами данных
ПО – программное обеспечение
ИБ – информационная безопасность
СМИБ – Система менеджмента информационной безопасности
Plan (планирование) – фаза создания СМИБ, создание перечня активов, оценки рисков и выбора мер
Do (действие) – этап реализации и внедрения соответствующих мер
Check (проверка) – фаза оценки эффективности и производительности СМИБ. Обычно выполняется внутренними аудиторами
Act (улучшения) – выполнение превентивных и корректирующих действий
Пользователь БД – программа или человек, обращающийся к БД на ЯМД
Запрос – процесс обращения пользователя к БД с целью ввода, получения или изменения информации в БД
Логическая структура БД – определение БД на физически независимом уровне, ближе всего соответствует концептуальной модели БД

Топология БД, структура распределенной БД – схема распределения физической БД по сети

Локальная автономность – означает, что информация локальной БД и связанные с ней определения данных принадлежат локальному владельцу и им управляются

Удаленный запрос – запрос, который выполняется с использованием модемной связи

Возможность реализации удаленной транзакции – обработка одной транзакции, состоящей из множества SQL-запросов на одном удаленном узле

Поддержка распределенной транзакции – допускает обработку транзакции, состоящей из нескольких запросов SQL, которые выполняются на нескольких узлах сети (удаленных или локальных), но каждый запрос в этом случае обрабатывается только на одном узле, то есть запросы не являются распределенными. При обработке одной распределенной транзакции разные локальные запросы могут обрабатываться в разных узлах сети

Распределенный запрос – запрос, при обработке которого используются данные из БД, расположенные в разных узлах сети

Глава I. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В первой части нашего учебно-методического пособия мы кратко останавливались на основных понятиях и определениях информационной безопасности.

Информация – результат и отражение в человеческом сознании, многообразие внутреннего и окружающего миров (сведения об окружающих человека предметах, явлений, действия других людей).

Информационная безопасность может рассматриваться в следующих значениях:

Состояние (качество) определённого объекта (в качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства, организации и т.п.).

Деятельность, направленная на обеспечение защищённого состояния объекта (в этом значении чаще используется термин «защита информации»).

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности (обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости) информации.

Информационная безопасность (англ. *information security*) – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, недоказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.

Безопасность информации (данных) (англ. *information (data) security*) – состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность. Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на дру-

гие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе. Безопасность информации (при применении информационных технологий) (англ. *IT security*) – состояние защищённости информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

Безопасность автоматизированной информационной системы – состояние защищённости автоматизированной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчётность и подлинность её ресурсов.

Информационная безопасность – защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Поддерживающая инфраструктура – системы электро-, тепло-, водо-, газоснабжения, системы кондиционирования и т. д., а также обслуживающий персонал. Неприемлемый ущерб – ущерб, которым нельзя пренебречь.

Г.М. Шушков, И.В. Сергеев определяют «информационную безопасность» как «процесс баланса между возникающими, воздействующими угрозами и успешностью противодействия этим угрозам со стороны органов государственной власти, отвечающих за безопасность государства».

Информационная безопасность государства – состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере. В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Также важным аспектом информационной безопасности является определение и классификация возможных угроз безопасности.

Ценность информации является важнейшим критерием при принятии решений о защите информации. Уровень секретности – административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю секретной конкурентной информации, регламентируемой специальным документом с учетом государственно-военной стратегической, коммерческих, служебных или частных интересов.

Статистика защиты информации показывает, что защищать нужно не только секретную информацию, но и связанную с ней не секретную.

Существенные признаки понятия:

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

- конфиденциальность (англ. *confidentiality*) – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право;
- целостность (англ. *integrity*) – избежание несанкционированной модификации информации;
- доступность (англ. *availability*) – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

- безотказность или апеллируемость (англ. *non-repudiation*) – способность удостоверять имевшее место действие или событие так, что эти события или действия не могли быть позже отвергнуты;
- подотчётность (англ. *accountability*) – свойство, обеспечивающее однозначное прослеживание действий любого логического объекта;
- достоверность (англ. *reliability*) – свойство соответствия предусмотренному поведению или результату;

- аутентичность или подлинность (англ. *authenticity*) – свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

1.1. Информация и информационная безопасность

Информация (лат. *informatio* – разъяснение, изложение), первоначально – сведения, передаваемые людьми устным, письменным или другим способом с помощью условных сигналов, технических средств и т.д. С середины XX века *информация* является общенаучным понятием, включающим в себя:

- сведения, передаваемые между людьми, человеком и автоматом, автоматом и автоматом;
- сигналы в животном и растительном мире;
- признаки, передаваемые от клетки к клетке, от организма к организму и т.д.

Другими словами, информация носит фундаментальный и универсальный характер, являясь многозначным понятием. Эту мысль можно подкрепить словами Н. Винера (отца кибернетики): «Информация есть информация, а не материя и не энергия».

Согласно традиционной философской точке зрения, информация существует независимо от человека и является свойством материи. В рамках рассматриваемой дисциплины под *информацией* (в узком смысле) мы будем понимать сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах.

Опираясь на это определение информации, рассмотрим понятия информационной безопасности и защиты информации.

В Доктрине информационной безопасности под термином *информационная безопасность* понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В более узком смысле под *информационной безопасностью* мы будем понимать состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамерен-

ных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Защита информации – комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.

Важно отметить, что информационная безопасность – это одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным состоянием (уровнем) защищенности, а защита информации – это процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы.

Рассмотрим более подробно составляющие этих определений.

Под *субъектами информационных отношений* понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры.

К *поддерживающей инфраструктуре* относятся не только компьютеры, но и помещения, системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Ущерб может быть *приемлемым* или *неприемлемым*. Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

Информационная угроза – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации.

Таким образом, концепция информационной безопасности, в общем случае, должна отвечать на три вопроса:

- Что защищать?
- От чего (кого) защищать?
- Как защищать?

Информационная система (автоматизированная информационная система) – это совокупность технических (аппаратных) и программных средств, а также работающих с ними пользователей (персонала), обеспечивающая информационную технологию выполнения установленных функций.

Жизненный цикл информационной системы – непрерывный процесс, начинающийся с момента принятия решения о создании информационной системы и заканчивающийся в момент полного изъятия ее из эксплуатации.

1.2. Основные составляющие информационной безопасности

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

Иногда в число основных составляющих информационной безопасности включают защиту от несанкционированного доступа (НСД) к информации, под которым понимают доступ к информации, нарушающий правила разграничения доступа с использование штатных средств. В то же время обеспечение конфиденциальности как раз и подразумевает защиту от НСД.

Мы дали определения основным составляющим информационной безопасности (доступность, целостность и конфиденциальность информации).

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность – какой смысл в информационной услуге, если она содержит искаженные сведения? Наконец, конфиденциальная информация есть как у организаций, так и отдельных пользователей.

Из всего выше приведенного следуют два следствия:

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

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

Штатные средства – совокупность программного и аппаратного обеспечения рассматриваемой информационной системы.

Транзакция – одно действие или их последовательность, выполняемых одним или несколькими пользователями (прикладными программами) с целью осуществления доступа или изменения информации, воспринимаемых как единое целое и переводящих ее из одного непротиворечивого (согласованного) состояния в другое непротиворечивое состояние.

1.3. Объекты защиты

Основными *объектами защиты* при обеспечении информационной безопасности являются:

- все виды информационных ресурсов. *Информационные ресурсы (документированная информация)* – информация, зафик-

сированная на материальном носителе с реквизитами, позволяющими ее идентифицировать;

- права граждан, юридических лиц и государства на получение, распространение и использование информации;

- система формирования, распространения и использования информации (информационные системы и технологии, библиотеки, архивы, персонал, нормативные документы и т.д.);

- система формирования общественного сознания (СМИ, социальные институты и т.д.).

Принято различать следующие средства защиты (рисунок 1.1):

Рисунок 1.1 – Классификация средств защиты

I. Формальные средства защиты – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.

Физические средства – механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно от информационных систем, создавая различного рода препятствия на пути дестабилизирующих факторов (замок на двери, жалюзи, забор, экраны).

Аппаратные средства – механические, электрические, электромеханические, электронные, электронно-механические, оптические, лазерные, радиолокационные и тому подобные устройства, встраиваемые в информационных системах или сопрягаемые с ней специально для решения задач защиты информации.

Программные средства – пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной

аппаратуры, однако они ведут к снижению производительности информационных систем, требуют выделения под их нужды определенного объема ресурсов и т.п.

К *специфическим средствам* защиты информации относятся криптографические методы. В информационных системах криптографические средства защиты информации могут использоваться как для защиты обрабатываемой информации в компонентах системы, так и для защиты информации, передаваемой по каналам связи. Само преобразование информации может осуществляться аппаратными или программными средствами, с помощью механических устройств, вручную и т.д.

II. Неформальные средства защиты – регламентируют деятельность человека.

Законодательные средства – законы и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Распространяются на всех субъектах информационных отношений. В настоящее время отношения в сфере информационной безопасности регулируются более чем 80 законами и нормативными документами, иногда достаточно противоречивыми.

Организационные средства – организационно-технические и организационно-правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы (строительство помещений, проектирование информационных систем, монтаж и наладка оборудования, испытания и эксплуатация информационных систем). Другими словами – это средства уровня организации, регламентирующие перечень лиц, оборудования, материалов и т.д., имеющих отношение к информационным системам, а также режимов их работы и использования. К организационным мерам также относят сертификацию информационных систем или их элементов, аттестацию объектов и субъектов на выполнение требований обеспечения безопасности и т.д.

Морально-этические средства – сложившиеся в обществе или в данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе, ведет к потере престижа и авторитета. Наиболее показательные пример – кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

Основные понятия информационной безопасности Залогом успешной сдачи экзамена CISSP является хорошее понимание концепции управления ин формационной безопасностью в организации. Прежде всего следует разобраться, что стоит за такими понятиями, как информационная безопасность, актив, угроза, уязвимость, контроль и риск. Под информационной безопасностью (ИБ) обычно понимают состояние (свойство) защищенности ресурсов информационной системы в условиях наличия угроз в информационной сфере. Защита информации – это процесс, направленный на обеспечение информационной безопасности. Определяющими факторами информационной безопасности являются угроза *(threat)* и риск *(risk)*. Угрозой называют потенциальную причину (событие, нарушение, инцидент), снижающую уровень информационной безопасности системы, т.е. потенциально способную привести к негативным последствиям *(impact)* и ущербу *(loss)* системы или организации. Риск представляет собой возможный ущерб, т.е. комбинацию (как правило, произведение) вероятности реализации угрозы и ущерба от нее. Отметим, что угроза и риск определяются не вообще, а относительно конкретного защищаемого ресурса. В терминологии менеджмента бизнес-процессов вместо ресурса используется синонимическое понятие – актив *(asset)*, под определение которого подпадает все, что имеет ценность для организации. В информационной сфере примерами активов являются: информация, программное обеспечение, аппаратное обеспечение, информационная система (сложный актив, включающий предыдущие), человек, имидж организации. В итоге, активами представляются все те объекты, которые подлежат защите путем выстраивания процессов информационной без опасности.

Таблица 1 – Сертификация специалистов
Вопросы кибер безопасности № 1(2) – 2014

Направления обеспечения безопасности	**Техногенные**		**Природные**
	Преднамеренные	**Случайные**	
Контроль физического доступа	Бомбардировка	Сон вахтерши	Торнадо
Сохранность оборудования	Вандализм	Запыление	Шаровые молнии
Управление коммуникациями	Прослушивание сети	Флуктуации в сети	Магнитные бури
Защита информационных хранилищ	Взлом парольной системы	Сбой криптосредств	Грибки
Управление непрерывностью деятельности	Последствие DOS – атаки	Последствия текстов на проникновение	Карстовые процессы
Соответствие законодательству	Компьютерное пиратство	Тиражирование персональных данных	Природные пожары

Угрозы классифицируют по ряду критериев:

- по причине возникновения (природные или техногенные, в том числе преднамеренные или случайные);
- по расположению источника (внешние или внутренние);
- по компрометируемой подсистеме или сегменту (сетевые, криптографические и др.);
- по этапу формирования в жизненном цикле системы (реализационные и эксплуатационные);
- по результирующему действию (нарушают целостность, конфиденциальность, доступность).

Примеры угроз представлены в таблице 1. Довольно подробные каталоги угроз подготовлены немецким федеральным агентством по информационной безопасности (BSI). Одной из основных угроз ИБ компьютерных систем является возможность реализации уязвимости *(vulnerability)* в ресурсах системы. Под уязвимостью понимают реализационный дефект («слабость»),

снижающий уровень защищенности ресурсов от тех или иных угроз. Отметим, наличие уязвимости становится угрозой, если ее можно реализовать так, что это приведет к недопустимому ущербу организации. Например, наличие сетевых уязвимостей в программном обеспечении изолированного компьютера не является угрозой. Умышленная реализация уязвимостей в компьютерных системах, приводящая к ущербу организации, называется атакой на ресурсы. Защищенность системы достигается обеспечением совокупности свойств ИБ ресурсов и инфраструктуры, основными из которых являются конфиденциальность *(confi dentiality)*, целостность *(integrity)*, доступность *(availability)*.

В зарубежных учебниках свойства конфиденциальности, целостности, доступности часто графически представляются в виде ссылки на треугольник CIA. *Конфиденциальность* – свойство системы, определяющее ее защищенность от несанкционированного раскрытия информации. *Целостность* – свойство, определяющее защищенность от несанкционированного изменения. Разделяют логическую и физическую целостность. Физическая целостность подразумевает неизменность физического состояния данных на машинном носителе. Логическая целостность отражает корректность выполнения процессов (транзакций), полноту и непротиворечивость информации, например, в СУБД, файловых системах, электронных архивах, хранилищах данных, системах управления документооборотом и т.д. *Доступность* – характеристика, определяющая возможность за приемлемое время получить требуемую информационную услугу авторизованному пользователю. С доступностью часто связывают такую характеристику системы как готовность – способность к выполнению заявленных функций в установленных технических условиях. Атаки, имеющие целью нарушить степень доступности, получили название атак на отказ в обслуживании (DOS-атаки). Кроме названных, часто в качестве наиболее важных свойств ИБ системы, для выражения значимости, упоминают аутентичность, подотчетность, недоказуемость, надежность и др.

Объём (реализация) понятия «информационная безопасность»

Системный подход к описанию информационной безопасности предлагает выделить следующие составляющие информационной безопасности:

1. Законодательная, нормативно-правовая и научная база.
2. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
3. Организационно-технические и режимные меры и методы (Политика информационной безопасности).
4. Программно-технические способы и средства обеспечения информационной безопасности.

Целью реализации информационной безопасности какого-либо объекта является построение Системы обеспечения информационной безопасности данного объекта (СОИБ). Для построения и эффективной эксплуатации СОИБ необходимо:

- выявить требования защиты информации, специфические для данного объекта защиты;
- учесть требования национального и международного Законодательства;
- использовать наработанные практики (стандарты, методологии) построения подобных СОИБ;
- определить подразделения, ответственные за реализацию и поддержку СОИБ;
- распределить между подразделениями области ответственности в осуществлении требований СОИБ;
- на базе управления рисками информационной безопасности определить общие положения, технические и организационные требования, составляющие Политику информационной безопасности объекта защиты;
- реализовать требования Политики информационной безопасности, внедрив соответствующие программно-технические способы и средства защиты информации;
- реализовать Систему менеджмента (управления) информационной безопасности (СМИБ);

- используя СМИБ организовать регулярный контроль эффективности СОИБ и при необходимости пересмотр и корректировку СОИБ и СМИБ.

Как видно из последнего этапа работ, процесс реализации СОИБ непрерывный и циклично (после каждого пересмотра) возвращается к первому этапу, повторяя последовательно все остальные. Так СОИБ корректируется для эффективного выполнения своих задач защиты информации и соответствия новым требованиям постоянно обновляющейся информационной системы.

Организационно-технические и режимные меры и методы

Для описания технологии защиты информации конкретной информационной системы обычно строится так называемая *Политика информационной безопасности* или Политика безопасности рассматриваемой информационной системы.

Политика безопасности (информации в организации) (англ. *Organizational security policy*) – совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Политика безопасности информационно-телекоммуникационных технологий (англ. *ICT security policy*) – правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и её информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию (рисунок 1.2).

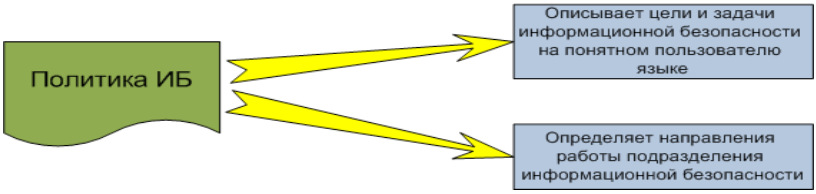


Рисунок 1.2 – Политика информационной безопасности

Для построения Политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы:

- защита объектов информационной системы;
- защита процессов, процедур и программ обработки информации;
- защита каналов связи (акустические, инфракрасные, проводные, радиоканалы и др.), включая защиту информации в локальных сетях;
- подавление побочных электромагнитных излучений;
- управление системой защиты.

При этом по каждому из перечисленных выше направлений Политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

1) определение информационных и технических ресурсов, подлежащих защите;

2) выявление полного множества потенциально возможных угроз и каналов утечки информации;

3) проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

4) определение требований к системе защиты;

5) осуществление выбора средств защиты информации и их характеристик;

6) внедрение и организация использования выбранных мер, способов и средств защиты;

7) осуществление контроля целостности и управление системой защиты.

Политика информационной безопасности оформляется в виде документированных требований на информационную систему. Документы обычно разделяют по уровням описания (детализации) процесса защиты.

Документы верхнего уровня Политики информационной безопасности отражают позицию организации к деятельности в области защиты информации, её стремление соответствовать государственным, международным требованиям и стандартам в этой области. Подобные документы могут называться «Концепция ИБ», «Регламент управления ИБ», «Политика ИБ», «Технический стандарт ИБ» и т.п. Область распространения документов

верхнего уровня обычно не ограничивается, однако данные документы могут выпускаться и в двух редакциях: для внешнего и внутреннего использования.

К среднему уровню относят документы, касающиеся отдельных аспектов информационной безопасности. Это требования на создание и эксплуатацию средств защиты информации, организацию информационных и бизнес-процессов организации по конкретному направлению защиты информации. Например, Безопасности данных, Безопасности коммуникаций, Использования средств криптографической защиты, Контентной фильтрации и т.п. Подобные документы обычно издаются в виде внутренних технических и организационных политик (стандартов) организации. Все документы среднего уровня политики информационной безопасности конфиденциальны.

В политику информационной безопасности нижнего уровня входят регламенты работ, руководства по администрированию, инструкции по эксплуатации отдельных сервисов информационной безопасности.

Повышение и обеспечение заданных уровней конфиденциальности, целостности и доступности ресурсов осуществляется путем применения мер (механизмов) безопасности, которые на профессиональном жаргоне часто называются контролями (от. англ. *controls* – инструменты/средства управления). Очень важно не путать этот жаргонизм с привычным словом «контроль», имеющим другое значение: наблюдение за поведением управляемой системы с целью обеспечения ее оптимального функционирования. Контроли могут иметь технический *(technical)*, организационный *(administrative)* и физический *(physical)* характер. Под понятием «технические контроли» совпадают программные и программно-аппаратные средства защиты, такие как антивирусы, межсетевые экраны, системы обнаружения вторжений, средства шифрования данных и т. п.

В качестве организационных контролей выступают правила, обязательные для исполнения сотрудниками. Например, наличие согласования заявки на предоставление доступа к системе у ее

владельца (как правило, руководителя бизнес-подразделения, отвечающего за процессы, которые поддерживаются данной системой). Хорошими примерами физических контролей являются двери, решетки, заборы, ограничивающие физический доступ к нашим активам. Контроли могут придерживаться различных целей, например, быть превентивными *(preventive)*, детективными *(detective)*, корректирующими *(corrective)*, восстанавливающими *(recovery)* и другими.

Более подробно контроли мы рассмотрим в следующей публикации, касающейся вопросов обеспечения безопасного доступа. Применение различных видов и типов контролей тесно связано с концепцией эшелонированной обороны *(defense in depth, multilevel security)*, представляющей идеологию проектирования систем защиты с несколькими уровнями мер (механизмов) безопасности, позволяющими обеспечить эффективную защиту даже в случае «пробивания» обороны на одном уровне. Управление информационной безопасностью Скоординированные действия, выполняемые с целью повышения и поддержания на требуемом уровне ИБ организации, называются управлением (менеджментом*) информационной безопасностью.

Термин «управление» в данном разделе тождественен понятию менеджмента, используемому в системах качества по ISO 9000. Система менеджмента информационной безопасности (СМИБ, ISMS) организации основывается на подходе бизнес-риска и предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ. В рамках СМИБ рассматривают структуру системы, политики, действия по планированию, обязанности, практики, процедуры, процессы и ресурсы организации.

В первую очередь необходимо определить контекст, в котором работает организация, и четко понимать потребности и ожидания всех сторон, заинтересованных в функционирующей системе управления информационной безопасностью. К заинтересованным сторонам можно отнести владельцев бизнеса, клиентов, партнеров, регулирующие органы, сотрудников и др. Важно,

что стандарт позволяет задать границы системы управления информационной безопасностью, то есть дает возможность внедрить СМИБ «вокруг» определенных критичных бизнес-процессов, а затем уже при необходимости расширять область действия СМИБ на другие процессы.

Внедрение СМИБ невозможно без реальной поддержки со стороны топ-менеджмента организации, определяющего четкую политику информационной безопасности, включающую цели и обязательства выполнять все применимые требования (законодательства, партнеров, клиентов и т.п.).

Методология должна быть разработана таким образом, чтобы его можно было повторить и получить сравнимые результаты. В ходе процесса анализа рисков необходимо в первую очередь идентифицировать риски ИБ *(risk identifi cation)* и определить владельцев рисков. Затем провести анализ рисков *(risk analysis)*, в ходе которого определить вероятность риска, размер ущерба и уровень рисков. После чего провести оценивание риска *(risk evaluation)* относительно установленных критериев принятия рисков и задать приоритеты для обработки рисков *(risk treatment)*.

Очень важно понимать, что подходы к оценке рисков предусматривают также оценку уязвимостей *(vulnerability assessment)* и существующих контролей *(control evaluation)* для минимизации угроз. Конкретные подходы к проведению оценки рисков информационной безопасности более подробно мы рассмотрим в следующем выпуске пособия. В отношении рисков, значения которых не соответствуют критериям принятия, важно определиться с решением относительно их обработки.

Помимо уже упомянутого принятия риска *(risk accepting)*, заключающегося в том, что организация соглашается с возможной реализацией угрозы и принимает последствия, вариантами обработки рисков являются:

- минимизация риска *(risk mitigation, reducing risk)* посредством внедрения контролей;

- передача риска *(assigning risk, transferring risk)*, которая может заключаться как в его страховании, так и передаче подрядчику (в совокупности с процессами, передающимися на аутсорсинг);

- избежание риска *(rejecting risk, avoiding risk)*, которое может заключаться в изменении процесса таким образом, что риск становится неактуальным.

Необходимо отметить, что в результате обработки риска остается так называемый остаточный риск *(residual risk)*, который принимается менеджментом компании (владельцами рисков). Внедрение контролей безопасности на практике для большинства выявленных рисков принимается решение об их минимизации путем внедрения контролей.

Контроль процессов в результате внедрения контролей должны быть получены работающие процессы СМИБ, которые выполняются, измеряются и контролируются. Необходимо отметить следующие три важных составляющих контроля работы СМИБ:

- операционный контроль;
- внутренний аудит;
- анализ со стороны руководства.

Операционный контроль подразумевает собой текущий контроль со стороны непосредственных руководителей. Например, принятая процедура предусматривает выполнение периодического сканирования на наличие уязвимостей сетевых сервисов, и отвечает за эту функцию конкретный специалист отдела ИБ. Соответственно руководитель отдела следит за тем, чтобы задача выполнялась подчиненным, и он вовремя получал отчет с результатами сканирования. Внутренний аудит заключается в периодической проверке эффективности контролей. Например, аудитор просит системного администратора предоставить перечень учетных записей, созданных в течение прошлого года, выбирает несколько и просит показать заявки, по которым он может убедиться, что доступ был согласован руководителями сотрудников и владельцами системы.

Анализ со стороны руководства подразумевает, что менеджмент интересуется тем, как работает СМИБ и, в частности, анализирует результаты проведенных аудитов (как внутренних, так и внешних), информацию о количестве произошедших инцидентов ИБ, в каком объеме требуются ресурсы для работы системы и т.п.

Следует помнить, что часто под политикой информационной безопасности *(information security policy)* понимается высокоуровневый документ, предназначенный для обеспечения управления ИБ в соответствии с требованиями бизнеса, партнеров, клиентов, законодательной базы.

Высокоуровневая политика безопасности, как правило, представляет собой достаточно статичный документ. Такой документ обычно содержит:

- общую информацию об обеспечении ИБ в организации (в которой мотивировано определена необходимость обеспечения и поддержки режима безопасности);
- заявление о поддержке *(commitment)* мероприятий по обеспечению ИБ на всех управленческих уровнях;
- основные положения по определению целей ИБ;
- распределение ролей и определение общей ответственности за реализацию мероприятий по обеспечению ИБ (в том числе по разработке и корректировке политик);
- ссылки на низкоуровневые документы, конкретно определяющие порядок реализации тех или иных аспектов, связанных с обеспечением ИБ.

Документированная политика ИБ должна быть утверждена руководством и доведена до сведения всех сотрудников организации и внешних сторон, к которым она относится. Кроме высокоуровневой политики выделяют низкоуровневые политики (частные политики, под политики), как правило, отражающие требования в определенной области (домене). В качестве примеров политик низкого уровня можно привести политику управления доступом, политику управления паролями, политику резервного копирования и т.п. Точный состав частных политик зависит от особенностей организации: ее размера, структуры, корпоративной культуры и т.п.

Руководства *(guidelines)* отличаются от стандартов в первую очередь тем, что носят рекомендательный характер. Руководства, в частности, могут определять, как именно следует реализовывать то или иное требование на практике с учётом локальной специфи-

ки. Так, например, специалист по информационной безопасности может разработать руководство, описывающее различные алгоритмы генерации надежных паролей, чтобы облегчить задачу выбора пароля пользователю. Процедура *(procedure)* представляют собой документ, определяющий последовательность действий по выполнению какой-либо задачи в соответствии с требованиями политик и стандартов. Из процедуры должно быть ясно, кто, что и когда делает. Хорошим примером процедуры является процедура регистрации пользователей в системе, описывающая этапы согласования заявки на доступ. Необходимо отметить, что, в основном, упомянутые документы ориентированы на специалистов отделов ИТ/ИБ, руководителей подразделений. Для неподготовленных сотрудников содержание данных документов может быть непонятным. В таких случаях разрабатывается документ «Свод правил для сотрудников», в котором доступным языком без использования технических терминов формулируются требования, которые должны выполнять сотрудники. Также функционал по обеспечению ИБ должен быть закреплен в положениях об отделах и должностных инструкциях. К отдельным видам документов стоит отнести так называемые записи *(records)*. Записи представляют собой те документы, которые создаются при выполнении процедуры, например, заявка на предоставление доступа к системе, журнал системы контроля доступа с информацией о том, кто входил в серверное помещение, и т.п.

В данном учебно-методическом пособии мы рассмотрели ключевые понятия менеджмента информационной безопасности, разобравшись в которых можно серьезно повысить свои шансы на успешную сдачу экзамена. Приоритетность изучения данной учебной информации обусловлена тем, что в пройденном разделе представлены основные понятия информационной безопасности, на которые мы будем ссылаться при публикации очередного учебного материала, так как в первой части нашего учебно-методического пособия мы детально рассмотрели подходы к оценке рисков информационной безопасности.

1.4. Программно-технические способы и средства обеспечения информационной безопасности

В литературе предлагается следующая классификация средств защиты информации:

- Средства защиты от несанкционированного доступа.
- Средства авторизации.
- Мандатное управление доступом.
- Избирательное управление доступом.
- Управление доступом на основе ролей.
- Журналирование (также называется Аудит).
- Системы анализа и моделирования информационных потоков (CASE-системы).
- Системы мониторинга сетей:

- системы обнаружения и предотвращения вторжений (IDS/IPS);

- системы предотвращения утечек конфиденциальной информации (DLP-системы);

- анализаторы протоколов.

- Антивирусные средства.
- Межсетевые экраны.
- Криптографические средства:

- шифрование;

- цифровая подпись.

- Системы резервного копирования.
- Системы бесперебойного питания:

- источники бесперебойного питания;

- резервирование нагрузки;

- генераторы напряжения.

- Системы аутентификации:

- пароль;

- ключ доступа (физический или электронный);

- сертификат;

- биометрия.

- Средства предотвращения взлома корпусов и краж оборудования.

- Средства контроля доступа в помещения.
- Инструментальные средства анализа систем защиты:

- антивирус.

Способы защиты от компьютерных злоумышленников

Информационная безопасность – это, прежде всего, защита сети от различного вида атак. Существует ряд простых средств, с помощью которых можно остановить попытки проникновения в сеть:

1. Оперативная установка исправлений для программ, работающих в интернете.

2. Антивирусные программы по обнаружению различного рода взломов и вирусов незаменимы для повышения безопасности любой сети. Они наблюдают за работой компьютеров и выявляют на них вредоносные программы.

3. Следует использовать наиболее надёжные пароли, менять их как можно чаще, и чтобы их длина была максимальной. Это может предотвратить кражу секретной и не секретной информации.

4. Соединения с удаленными машинами (компьютерами) должны быть защищены с помощью паролей, чтобы избежать проникновения в сеть с помощью прослушивания сетевого трафика в наиболее важных местах и выделения из него имен пользователей и их паролей.

5. При установке новой операционной системы обычно разрешаются все сетевые средства, что является не безопасным. Кроме перечисленных выше средств защиты существует еще множество способов предотвращения взломов и краж информации. Для избегания неприятных ситуаций необходимо изучать рекомендации по безопасности и придерживаться необходимых средств защиты.

1.5. Исторические аспекты возникновения и развития информационной безопасности

- I этап – до 1916 года – характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.
- II этап – начиная с 1916 года – связан с началом использования искусственно создаваемых технических средств электро и радиосвязи. Для обеспечения скрытности и помехозащищённости радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).
- III этап – начиная с 1935 года – связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищённости радиолокационных средств от воздействия на их приёмные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.
- IV этап – начиная с 1946 года – связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.
- V этап – начиная с 1965 года – обусловлен созданием и развитием локальных информационно-коммуникацион-

ных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

- VI этап – начиная с 1973 года – связан с использованием сверх мобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьёзнее. Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Образовались сообщества людей – хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности – важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право – новая отрасль международной правовой системы.
- VII этап – начиная с 1985 года – связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить, что очередной этап развития информационной безопасности, очевидно, будет связан с широким использованием сверх мобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

Цели оценки информационной безопасности:

- определить ценность информационных активов;
- определить угрозы для конфиденциальности, целостности, доступности и/или идентифицируемый этих активов;
- определить существующие уязвимые места в практической деятельности организации;
- установить риски организации в отношении информационных активов;
- предложить изменения в существующей практике работы, которые позволят сократить величину рисков до допустимого уровня;
- обеспечить базу для создания проекта обеспечения безопасности.

Пять основных видов оценки:

1) Оценка уязвимых мест на системном уровне. Компьютерные системы исследованы на известные уязвимости и простейшие политики соответствия техническим требованиям.

2) Оценка на сетевом уровне. Произведена оценка существующей компьютерной сети и информационной инфраструктуры, выявлены зоны риска.

3) Общая оценка риска в рамках организации. Произведен анализ всей организации с целью выявления угроз для ее информационных активов.

4) Аудит. Исследована существующая политика и соответствие организации этой политике.

5) Испытание на возможность проникновения. Исследована способность организации реагировать на смоделированное проникновение.

При проведении оценки должны быть исследованы такие документы, как:

- политика безопасности;
- информационная политика;
- политика и процедуры резервного копирования;
- справочное руководство работника или инструкции;
- процедуры найма-увольнения работников;

- методология разработки программного обеспечения;
- методология смены программного обеспечения;
- телекоммуникационные политики;
- диаграммы сети.

Получив вышеуказанные политики и процедуры, каждая из них исследуется на предмет значимости, правомерности, завершенности и актуальности, так как политики и процедуры должны соответствовать цели, определенной в документе.

После оценки необходимо заняться разработкой политик и процедур, которые определяют предполагаемое состояние безопасности и перечень необходимых работ. Нет политики – нет плана, на основании которого организация разработает и выполнит эффективную программу ИБП.

Необходимо разработать следующие политики и процедуры:

- Информационная политика. Выявляет секретную информацию и способы ее обработки, хранения, передачи и уничтожения.
- Политика безопасности. Определяет технические средства управления для различных компьютерных систем.
- Политика использования. Обеспечивает политику компании по использованию компьютерных систем.
- Политика резервного копирования. Определяет требования к резервным копиям компьютерных систем.
- Процедуры управления учетными записями. Определяют действия, выполняемые при добавлении или удалении пользователей.
- План на случай чрезвычайных обстоятельств. Обеспечивает действия по восстановлению оборудования компании после стихийных бедствий или инцидентов, произошедших по вине человека.

Реализация политики безопасности заключается в реализации технических средств и средств непосредственного контроля, а также в подборе штата безопасности. Могут потребоваться изменения в конфигурации систем, находящихся вне компетенции отдела безопасности, поэтому в проведении программы безопасности должны участвовать системные и сетевые администраторы.

Система *менеджмента информационной безопасности* ... Plan (планирование) – фаза создания СМИБ, создание перечня активов, оценки рисков и выбора мер; Do (действие) – этап реализации и внедрения соответствующих мер; Check (проверка) – фаза оценки эффективности и производительности СМИБ.

Система менеджмента информационной безопасности (СМИБ) – часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и улучшении информационной безопасности.

В случае построения основывается на модели:

- Plan (планирование);
- Do (действие);
- Check (проверка);
- Act (улучшения).

Глава II. КРИПТОГРАФИЯ

О важности сохранения информации в тайне знали уже в древние времена, когда с появлением письменности появилась и опасность прочтения ее нежелательными лицами. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. С широким распространением письменности криптография стала формироваться как самостоятельная наука. В документах древних цивилизаций – Индии, Египта, Месопотамии – есть сведения о системах и способах составления шифрованных писем.

Точное время возникновения этих способов обмена тайной информацией теряется в глубине веков, и установить его невозможно. Историки полагают, что первые прото-криптографические приемы появились в Древнем Египте около 4 тыс. лет назад. Писцы, составлявшие жизнеописания правителей, стремились придать стандартным иероглифам необычный вид на монументах и гробницах, чтобы сообщить надписям менее обыденный и более почтительный стиль. Жрецы пользовались этим же приемом при переписывании религиозных текстов, чтобы те выглядели для мирян загадочнее и внушительнее. Такие «переводы» становились все менее понятными простому люду, который в результате оказывался во все большей зависимости от жрецов.

По мере развития египетской цивилизации ширилось использование иероглифов. С увеличением количества надписей, высекавшихся на стенах храмов, люди теряли к ним интерес. Египтологи считают, что писцы тогда стали еще больше видоизменять некоторые знаки в стремлении пробудить любопытство и привлечь внимание населения. Эти модификации никоим образом не были кодами или шифрами, но они заключали в себе два основных принципа криптологии, а именно: изменение письма и сокрытие его смысла. Бесспорных доказательств, указывающих на широкое использование модификаций иероглифов для сокрытия дипломатических, торговых или военных планов в Древнем Египте, нет.

Более явные криптологические примеры дошли до нас от цивилизаций Месопотамии – от вавилонян, ассирийцев, халдеев, использовавших особую систему письма – клинопись. В 1500 г. до н. э. на глиняной табличке был записан тщательно охраняемый рецепт глазури для гончарных изделий. Знаки, определяющие необходимые ингредиенты, были намеренно перемешаны. Таким образом, мы имеем право утверждать, что эта табличка является самой ранней известной секретной записью.

Криптография (от др.-греч. *κρυπτός* «скрытый» + *γράφω* «пишу») – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифровывание и расшифровывание проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптография не занимается защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищённых системах передачи данных.

Криптография – одна из старейших наук, её история насчитывает несколько тысяч лет.

2.1. История криптографии

Примерно с 500 г. до н. э. в Индии также широко применялись секретные записи, в частности в донесениях шпионов

и текстах, предположительно использовавшихся Буддой. Методы засекречивания включали в себя фонетическую замену, когда согласные и гласные менялись местами, использование перевернутых букв и запись текста под случайными углами. Различные индийские трактаты, ярким примером которых является «Артхашастра» (около 321–300 гг. до н. э.), показывают, что индийцы были хорошо знакомы со способами сокрытия информации.

Рассмотрим проблему тайной передачи информации и ее сокрытия от злоумышленника на расстоянии. Путей ее решения существует множество, среди которых можно выделить три основных направления:

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.

2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.

3. Использовать общедоступный канал связи, но передавать по нему нужную информацию в таком преобразованном виде, чтобы восстановить ее мог только адресат.

Проанализируем эти возможности.

С древних времен практиковалась охрана документа (носителя информации) физическими лицами, передача его специальным курьером (человеком (дипломатом) или животным (голубиная почта) и т.д. Но документ можно выкрасть, курьера можно перехватить, подкупить, в конце концов, убить. В настоящий момент для реализации данного механизма защиты используются современные телекоммуникационные каналы связи. Однако следует заметить, что данный подход требует значительных капитальных вложений. При современном уровне развития науки и техники сделать такой канал связи между удаленными абонентами для многократной передачи больших объемов информации практически нереально.

4. Разработкой средств и методов скрытия факта передачи сообщения занимается ***стеганография.*** Первые следы стеганографических методов теряются в глубокой древности. Так, в трудах древнегреческого историка Геродота встречается описание двух методов сокрытия информации: на обритую голову раба за-

писывалось необходимое сообщение, а когда его волосы отрастали, он отправлялся к адресату, который вновь брил его голову и считывал доставленное сообщение. Второй способ заключался в следующем: сообщение наносилось на деревянную дощечку, а потом она покрывалась воском, и, тем самым, не вызывала никаких подозрений. Потом воск соскабливался, и сообщение становилось видимым. В настоящий момент стеганографические методы в совокупности с криптографическими нашли широкое применение в целях сокрытия и передачи конфиденциальной информации.

Разработкой методов преобразования информации с целью ее защиты от несанкционированного прочтения занимается ***криптография.***

В истории развития криптографии можно выделить три этапа:

- наивная криптография;
- формальная криптография;
- математическая криптография.

Наивная криптография. Для наивной криптографии (до начала XVI в.) характерно использование любых, обычно примитивных, способов запутывания противника относительно содержания передаваемых сообщений.

На начальном этапе для защиты информации использовались методы кодирования и стеганографии, которые родственны, но не тождественны криптографии. Шифровальные системы сводились к использованию перестановки или замены букв на различные символы (другие буквы, знаки, рисунки, числа и т.п.). Одни и те же способы шифрования использовались повторно, ключи были короткими, использовались примитивные способы преобразования исходной информации в зашифрованное сообщение. Это позволяло, однажды установив алгоритм шифрования, быстро расшифровывать сообщения.

Одним из первых зафиксированных примеров является шифр Цезаря, состоящий в замене каждой буквы исходного текста на другую, отстоящую от нее в алфавите на определенное число позиций. Другой шифр, полибианский квадрат, авторство которого приписывается греческому писателю Полибию, является

шифром простой однозначной замены. В квадрат выписывались буквы алфавита (для греческого алфавита размер составлял 5x5). Каждая буква исходного текста заменялась на пару цифр – номер строки и столбца на пересечении которых стояла шифруемая буква.

С VIII века н. э. развитие криптографии происходит в основном в арабских странах. Считается, что арабский филолог Халиль аль-Фарахиди первым обратил внимание на возможность использования стандартных фраз открытого текста для дешифрования. Он предположил, что первыми словами в письме на греческом языке византийскому императору будут «Во имя Аллаха», что позволило ему прочитать оставшуюся часть сообщения. Позже он написал книгу с описанием данного метода – «Китаб аль-Муамма» («Книга тайного языка»). В 855 г. выходит «Книга о большом стремлении человека разгадать загадки древней письменности» арабского учёного Абу Бакр Ахмед ибн Али Ибн Вахшия ан-Набати, одна из первых книг о криптографии с описаниями нескольких шифров, в том числе с применением нескольких алфавитов. Также к IX веку относится первое известное упоминание о частотном криптоанализе – в книге Ал-Кинди «Манускрипт о дешифровке криптографических сообщений». В 1412 г. выходит 14-томная энциклопедия Шихаба ал-Калкашанди «Субх ал-Ааша», один из разделов которой «Относительно сокрытия в буквах тайных сообщений» содержал описание семи шифров замены и перестановки, частотного криптоанализа, а также таблицы частоты появления букв в арабском языке на основе текста Корана. В словарь криптологии арабы внесли такие понятия как алгоритм и шифр.

В древние времена широкое применение нашли различные простейшие криптографические устройства.

Греческим поэтом Архилохом, жившим в VII веке до н. э. упоминается устройство под названием ***сцитала*** (греч. *σκυτάλη* – жезл). Достоверно известно, что сцитала (рисунок 2.1) использовалась в войне Спарты против Афин в конце V века до н. э. Она представляет собой цилиндр (иногда жезл командующего)

и узкую полоску пергамента, обматывавшуюся вокруг него по спирали, на которой в свою очередь писалось сообщение.

Рисунок 2.1 – Сцитала

Шифруемый текст писался на пергаментной ленте по длине палочки, после того как длина палочки оказывалась исчерпанной, она поворачивалась и текст писался далее, пока либо не заканчивался текст, либо не исписывалась вся пергаментная лента. В последнем случае использовался очередной кусок пергаментной ленты. Для расшифровки адресат использовал палочку такого же диаметра, на которую он наматывал пергамент, чтобы прочитать сообщение. Античные греки и спартанцы в частности, использовали этот шифр для связи во время военных кампаний. Однако такой шифр может быть легко взломан. Например, метод взлома сциталы был предложен ещё Аристотелем. Он состоит в том, что, не зная точного диаметра палочки, можно использовать конус, имеющий переменный диаметр и перемещать пергамент с сообщением по его длине до тех пор, пока текст не начнёт читаться – таким образом дешифруется диаметр сциталы.

Другим широко известным криптографическим устройством защиты информации был «диск Энея» – инструмент для защиты информации, придуманный Энеем Тактиком в IV веке до н. э. Устройство представляло собой диск диаметром 13–15 см и толщиной 1–2 см с проделанными в нём отверстиями, количество которых равнялось числу букв в алфавите. Каждому отверстию ставилась в соответствие конкретная буква. В центре диска находилась катушка с намотанной на неё ниткой.

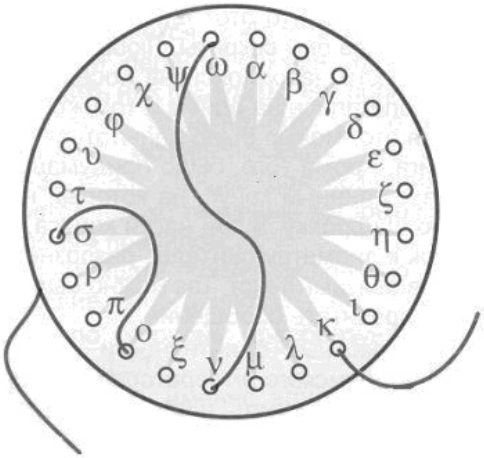


Рисунок 2.2 – Диск Энея

Механизм шифрования был очень прост. Чтобы зашифровать послание, необходимо было поочерёдно протягивать свободный конец нити через отверстия обозначающие буквы исходного не зашифрованного сообщения. В итоге, сам диск с продетой в его отверстия ниткой и являлся зашифрованным посланием. Получатель сообщения последовательно вытягивал нить из каждого отверстия, тем самым получал последовательность букв. Но эта последовательность являлась обратной по отношению к исходному сообщению, то есть он читал сообщение наоборот. Зашифрованное сообщение было доступно к прочтению любому, кто смог завладеть диском. Так как сообщение предавали обычные гонцы, а не воины, Эней предусмотрел возможность быстрого уничтожения передаваемой информации. Для этого было достаточно вытянуть всю нить за один из её концов, либо сломать диск, просто наступив на него. На самом деле «диск Энея» (рисунок 2.2) нельзя назвать настоящим криптографическим инструментом, поскольку прочитать сообщение мог любой желающий. Но это устройство стало прародителем первого по истине криптографического инструмента, изобретение которого также принадлежит Энею.

Прибор получил название «Линейка Энея». Она представляла собой устройство, имеющее отверстия, количество которых равнялось количеству букв алфавита. Каждое отверстие обозначалось своей буквой; буквы по отверстиям располагались в произвольном порядке. К линейке была прикреплена катушка с намотанной на неё ниткой. Рядом с катушкой имелась прорезь. При шифровании нить протягивалась через прорезь, а затем через отверстие, соответствующее первой букве шифруемого текста, при этом на нити завязывался узелок в месте прохождения её через отверстие; затем нить возвращалась в прорезь и аналогично зашифровывалась вторая буква текста, и т.д. После окончания шифрования нить извлекалась и передавалась получателю сообщения. Получатель, имея идентичную линейку, протягивал нить через прорезь до отверстий, определяемых узлами, и восстанавливал исходный текст по буквам отверстий. Такой шифр является одним из примеров шифра замены: когда буквы заменяются на расстояния между узелками с учетом прохождения через прорезь. Ключом шифра являлся порядок расположения букв по отверстиям в линейке. Посторонний, получивший нить (даже имея линейку, но без нанесенных на ней букв), не сможет прочитать передаваемое сообщение.

Формальная криптография. Этап формальной криптографии (конец XV – начало XX вв.) связан с появлением формализованных и относительно стойких к ручному криптоанализу шифров. В европейских странах это произошло в эпоху Возрождения, когда развитие науки и торговли вызвало спрос на надежные способы защиты информации.

К концу XIV в. между итальянскими городами-государствами в переписке уже применялись «номенклаторы»[1] (лат. *nomen* – «имя» и *calator* – «раб», «слуга»). Они состояли из кодовых обозначений для слогов, слов и имен, а также алфавитов шифрозамен. Вплоть до XIX в. номенклаторы оставались самой широко используемой системой сокрытия содержания сообщений.

[1] Первоначально номенклатором назывался раб, который обязан был знать и называть своему господину имена граждан города и всех рабов в доме, а также провозглашать названия подаваемых кушаний.

Симеоне де Крема (Simeone de Crema) был первым (1401 г.), кто использовал таблицы омофонов для сокрытия частоты появления гласных в тексте при помощи более чем одной шифрозамены (шифры многозначной замены).

Отцом западной криптографии называют учёного эпохи Возрождения Леона Баттисту Альберти. Изучив методы вскрытия использовавшихся в Европе моноалфавитных шифров (шифров однозначной замены), он попытался создать шифр, который был бы устойчив к частотному криптоанализу. Его «Трактат о шифре» был представлен в папскую канцелярию в 1466 г. и считается первой научной работой по криптографии. Он предложил вместо единственного секретного алфавита, как в моноалфавитных шифрах, использовать два или более, переключаясь между ними по какому-либо правилу. Однако флорентийский учёный так и не смог оформить своё открытие в полную работающую систему, что было сделано уже его последователями (Блез Вижинер). Другой печатной работой, в которой обобщены и сформулированы известные на тот момент алгоритмы шифрования, является труд «Полиграфия» (1518 г.) немецкого аббата Иоганна Трисемуса (Тритемия). Он же первым заметил, что шифровать можно и по две буквы за раз – биграммами (хотя первый биграммный шифр Playfair был предложен лишь в XIX веке).

В 1550 г. итальянский математик Джероламо Кардано, состоящий на службе у папы римского, предложил новую технику шифрования – решётку Кардано. Этот способ сочетал в себе как стеганографию (искусство скрытого письма), так и криптографию. Затруднение составляло даже понять, что сообщение содержит зашифрованный текст, а расшифровать его, не имея ключа (решётки), в то время было практически невозможно. Решётку Кардано считают первым транспозиционным шифром, или, как ещё называют, геометрическим шифром, основанным на положении букв в шифротексте.

Значительный толчок криптографии дало изобретение телеграфа. Сама передача данных перестала быть секретной, и сообщение, в теории, мог перехватить кто угодно. Интерес к криптографии возрос, в том числе, и среди простого населения,

в результате чего многие попытались создать индивидуальные системы шифрования. Преимущество телеграфа было явным и на поле боя, где командующий должен был отдавать немедленные приказы на поле сражения, а также получать информацию с мест событий. Это послужило толчком к развитию полевых шифров.

В 1863 г. Фридрих Касиски (англ. Friedrich Kasiski) опубликовал метод, впоследствии названный его именем, позволявшим быстро и эффективно вскрывать практически любые шифры того времени, в т.ч. полиалфавитные. Метод состоял из двух частей – определение периода шифра и дешифровка текста с использованием частотного криптоанализа.

В 1883 г. голландец Огюст Керкгоффс[1] опубликовал труд под названием «Военная криптография» (фр. «La Cryptographie Militaire»). В нём он описал шесть требований, которым должна удовлетворять защищённая система. Хотя к некоторым из них стоит относиться с подозрением, стоит отметить труд за саму попытку:

1) шифр должен быть физически, если не математически, не вскрываемым;

2) система не должна требовать секретности, на случай, если она попадёт в руки врага;

3) ключ должен быть простым, храниться в памяти без записи на бумаге, а также легко изменяемым по желанию корреспондентов;

4) зашифрованный текст должен (без проблем) передаваться по телеграфу;

5) аппарат для шифрования должен быть легко переносимым, работа с ним не должна требовать помощи нескольких лиц;

6) аппарат для шифрования должен быть относительно прост в использовании, не требовать значительных умственных усилий или соблюдения большого количества правил.

[1] Огюст Керкгоффс (Auguste Kerckhoffs, 1835–1903 гг.) – голландский лингвист и криптограф, профессор Парижской высшей школы коммерции во второй половине XIX века. В русских источниках встречаются разные переводы фамилии – Керкхофф, Кирхгоф, Керкгоффс, Керхофс, Керкхоффс. Полное имя, полученное при крещении, – Жан Вильгельм Губерт Виктор Франсуа Александр Огюст Керкгоффс фон Ниувенгоф.

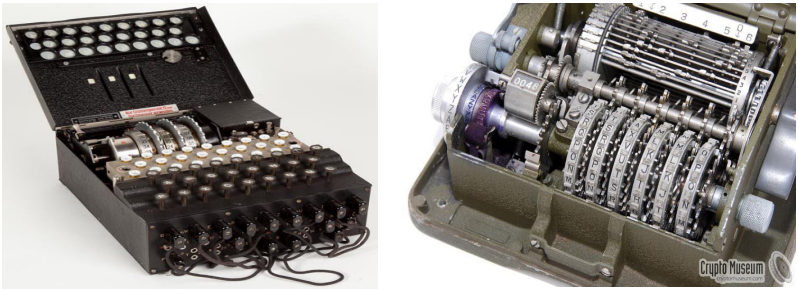
Им же был сформулирован известный «принцип Керкгоффса» – правило разработки криптографических систем, согласно которому в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым. Другими словами, при оценке надёжности шифрования необходимо предполагать, что противник знает об используемой системе шифрования всё, кроме применяемых ключей.

В 1920 г. вышла монография американского криптографа российского происхождения Уильяма Ф. Фридмана «Индекс совпадения и его применение в криптографии» (англ. «Index of Coincidence and Its Applications in Cryptography»). Работа вышла в открытой печати, несмотря на то, что была выполнена в рамках военного заказа. Двумя годами позже Фридман ввёл в научный обиход термины криптология и криптоанализ.

Криптография оказала влияние и на литературу. Упоминания о криптографии встречаются ещё во времена Гомера и Геродота, хотя они описывали искусство шифрования в контексте различных исторических событий. Первым вымышленным упоминанием о криптографии можно считать роман «Гаргантюа и Пантагрюэль» французского писателя XVI в. Франсуа Рабле, в одной из глав которого описываются попытки чтения зашифрованных сообщений. Упоминание встречается и в «Генрихе V» Шекспира. Впервые как центральный элемент художественного произведения криптография используется в рассказе «Золотой жук» Эдгара Аллана По 1843 г. В нём писатель не только показывает способ раскрытия шифра, но и результат, к которому может привести подобная деятельность – нахождение спрятанного сокровища. Одним из лучших описаний применения криптографии является рассказ 1903 г. Артура Конан Дойля «Пляшущие человечки». В рассказе великий сыщик Шерлок Холмс сталкивается с разновидностью шифра, который не только прячет смысл написанного, но, используя символы, похожие на детские картинки, скрывает сам факт передачи секретного сообщения. В рассказе герой успешно применяет частотный анализ, а также предположения

о структуре и содержании открытых сообщений для разгадывания шифра.

Перед началом Второй мировой войны ведущие мировые державы имели электромеханические шифрующие устройства, результат работы которых считался не вскрываемым. Эти устройства делились на два типа – роторные машины и машины на цевочных дисках (рисунок 2.3). К первому типу относят «Энигму», использовавшуюся войсками Германии и её союзников, второго типа – американская *М-209*. В СССР производились оба типа машин.



Энигма (Германия) М-209 (США)

Рисунок 2.3 – Шифровальные устройства

Успешные криптоатаки на подобного рода криптосистемы стали возможны только с появлением ЭВМ.

Математическая криптография. После Первой мировой войны правительства стран засекретили все работы в области криптографии. К началу 1930-х годов окончательно сформировались разделы математики, являющиеся основой для будущей науки: общая алгебра, теория чисел, теория вероятностей и математическая статистика. К концу 1940-х годов построены первые программируемые счётные машины, заложены основы теории алгоритмов, кибернетики. Тем не менее, в период после Первой мировой войны и до конца 1940-х годов в открытой печати было опубликовано совсем немного работ и монографий, но и те отражали далеко не самое актуальное состояние дел. Наибольший прогресс в криптографии достигается в военных ведомствах.

Ключевой вехой в развитии криптографии является фундаментальный труд Клода Шеннона «Теория связи в секретных

системах» (англ. Communication Theory of Secrecy Systems) – секретный доклад, представленный автором в 1945 г., и опубликованный им в «Bell System Technical Journal» в 1949 г. В этой работе, по мнению многих современных криптографов, был впервые показан подход к криптографии в целом как к математической науке.

В 1960-х годах начали появляться различные блочные шифры, которые обладали большей криптостойкостью по сравнению с результатом работы роторных машин. Однако они предполагали обязательное использование цифровых электронных устройств – ручные или полумеханические способы шифрования уже не использовались.

В 1967 г. выходит книга Дэвида Кана «Взломщики кодов». Хотя книга не содержала сколько-нибудь новых открытий, она подробно описывала имеющиеся на тот момент результаты в области криптографии, большой исторический материал, включая успешные случаи использования криптоанализа, а также некоторые сведения, которые правительство США полагало всё ещё секретными. Но главное – книга имела заметный коммерческий успех и познакомила с криптографией десятки тысяч людей. С этого момента начали понемногу появляться работы и в открытой печати.

Примерно в это же время Хорст Фейстель переходит из Военно-воздушных сил США на работу в лабораторию корпорации IBM. Там он занимается разработкой новых методов в криптографии и разрабатывает ячейку Фейстеля, являющуюся основой многих современных шифров, в том числе шифра Lucifer, ставшего прообразом шифра *DES* – бывшего стандарта шифрования США, первого в мире открытого государственного стандарта на шифрование данных. На основе ячейки Фейстеля были созданы и другие блочные шифры, в том числе TEA (1994 г.), Twofish (1998 г.), IDEA (2000 г.), а также ГОСТ 28147-89, являющийся стандартом шифрования в России.

В 1976 г. публикуется работа Уитфилда Диффи и Мартина Хеллмана «Новые направления в криптографии» (англ. «New

Directions in Cryptography»). Данная работа открыла новую область в криптографии, теперь известную как криптография с открытым ключом. Также в работе содержалось описание алгоритма Диффи-Хеллмана-Меркла, позволявшего сторонам сгенерировать общий секретный ключ, используя открытый канал связи. Хотя работа Диффи-Хеллмана создала большой теоретический задел для открытой криптографии, первой реальной криптосистемой с открытым ключом считают алгоритм RSA (названный по имени авторов – Рон Ривест (R. Rivest), Ади Шамир (A. Shamir) и Леонард Адлеман (L. Adleman)). Опубликованная в августе 1977 г., работа позволила сторонам обмениваться секретной информацией, не имея заранее выбранного секретного ключа. Стоит отметить, что и алгоритм Диффи-Хеллмана-Меркла, и RSA были впервые открыты в английских спецслужбах, но не были ни опубликованы, ни запатентованы из-за секретности.

В России для шифрования с открытым ключом стандарт отсутствует, однако для электронной цифровой подписи (органически связанной с шифрованием с открытым ключом) принят ГОСТ Р 34.10-2001, использующий криптографию на эллиптических кривых.

Создание асимметричных криптосистем подтолкнуло математиков и криптоаналитиков к изучению способов факторизации, дискретного логарифмирования, операций над эллиптическими кривыми в конечном поле и т.д.

Относительно новым методом является вероятностное шифрование. Вероятностное шифрование предложили Шафи Гольдвассер (Goldwasser) и Сильвио Микэли (Micali). Шифрование было названо «вероятностным» в связи с тем, что один и тот же исходный текст при шифровании с использованием одного и того же ключа может преобразовываться в совершенно различные шифротексты. При использовании криптосистем с открытым ключом существует возможность подбора открытого текста сопоставлением перехваченного шифротекста с результатом шифрования. Вероятностное шифрование позволяет на порядки увеличить сложность такого вида атаки.

Чарльз Беннет (Charles Bennet) и Жиль Брассард (Gilles Brassard), опираясь на работу Стивена Уиснера (Stephen Wiesner), разработали теорию квантовой криптографии, которая базируется скорее на квантовой физике, нежели на математике. Процесс отправки и приёма информации выполняется посредством объектов квантовой механики (например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи). Основанная на принципах квантовой механики, эта система, в отличие от обычной криптографии, теоретически позволяет гарантированно защитить информацию от злоумышленника, даже если тот обладает самой современной технологией и неограниченными вычислительными мощностями. На данный момент разрабатываются только прототипы квантовых криптосистем.

В то же время эффекты квантовой физики, возможно, смогут использоваться и для криптоанализа. Если будут построены квантовые компьютеры, то это поставит под вопрос существование современной криптографии.

Применение криптографии в решении вопросов аутентификации, целостности данных, передачи конфиденциальной информации по каналам связи и т.п. стало неотъемлемым атрибутом информационных систем. В современном мире криптография находит множество различных применений: она используется в сотовой связи, платном цифровом телевидении, при подключении к Wi-Fi, для защиты билетов от подделок на транспорте, в банковских операциях, в системах электронных платежей и т.д.

Глава III. БАЗА ДАННЫХ

Базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

Общепризнанная единая формулировка понятия БД отсутствует. Часто используются следующие отличительные признаки:

- БД хранится и обрабатывается в вычислительной системе. Таким образом, любые вне компьютерного хранилища информации (архивы, библиотеки, картотеки и т. п.) базами данных не являются.
- Данные в БД логически структурированы (систематизированы) с целью обеспечения возможности их эффективного поиска и обработки в вычислительной системе. Структурированность подразумевает явное выделение составных частей (элементов), связей между ними, а также типизацию элементов и связей, при которой с типом элемента (связи) соотносится определённая семантика и допустимые операции.
- БД включает метаданные, описывающие логическую структуру БД в формальном виде (в соответствии с некоторой метамоделью).

Из перечисленных признаков только первый является строгим, а другие допускает различные трактовки и различные степени оценки. Можно лишь установить некоторую степень соответствия требованиям к БД.

В такой ситуации не последнюю роль играет общепринятая практика. В соответствии с ней, например, не называют базами данных файловые архивы, Интернет-порталы или электронные таблицы, несмотря на то что они в некоторой степени обладают признаками БД. Принято считать, что эта степень в большинстве случаев недостаточна (хотя могут быть исключения).

Распространенная ошибка – некорректное использование термина «база данных» вместо термина «система управления базами данных». Эти понятия необходимо различать! (рисунок 3.1).

Рисунок 3.1 – Схема базы данных движка Mediawiki

Многие специалисты указывают на распространённую ошибку, состоящую в некорректном использовании термина «база данных» вместо термина «система управления базами данных», и указывают на необходимость различения этих понятий.

Проблемы определения.

В литературе предлагается множество определений понятия «база данных», отражающих скорее субъективное мнение тех или иных авторов, однако общепризнанная единая формулировка отсутствует.

Определения из международных стандартов:

- **База данных** – совокупность данных, хранимых в соответствии со схемой данных, манипулирование которыми выполняют в соответствии с правилами средств моделирования данных.
- **База данных** – совокупность данных, организованных в соответствии с концептуальной структурой, описывающей характеристики этих данных и взаимоотношения между ними, причём такое собрание данных, которое поддерживает одну или более областей применения.

Определения из авторитетных монографий:

- **База данных** – организованная в соответствии с определёнными правилами и поддерживаемая в памяти компьютера совокупность данных, характеризующая актуальное

состояние некоторой предметной области и используемая для удовлетворения информационных потребностей пользователей.

- **База данных** – некоторый набор перманентных (постоянно хранимых) данных, используемых прикладными программными системами какого-либо предприятия.
- **База данных** – совместно используемый набор логически связанных данных (и описание этих данных), предназначенный для удовлетворения информационных потребностей организации.

В определениях наиболее часто (явно или неявно) присутствуют следующие отличительные признаки:

1. *БД хранится и обрабатывается в вычислительной системе.* Таким образом, любые вне компьютерные хранилища информации (архивы, библиотеки, картотеки и т. п.) базами данных не являются.

2. *Данные в БД логически структурированы (систематизированы)* с целью обеспечения возможности их эффективного поиска и обработки в вычислительной системе.

Структурированность подразумевает явное выделение составных частей (элементов), связей между ними, а также типизацию элементов и связей, при которой с типом элемента (связи) соотносится определённая семантика и допустимые операции.

3. *БД включает схему, или метаданные*, описывающие логическую структуру БД в формальном виде (в соответствии с некоторой метамоделью).

Из перечисленных признаков только первый является строгим, а другие допускают различные трактовки и различные степени оценки. Можно лишь установить некоторую степень соответствия требованиям к БД.

В такой ситуации не последнюю роль играет общепринятая практика. В соответствии с ней, например, не называют базами данных *файловые архивы, Интернет-порталы* или *электронные таблицы*, несмотря на то, что они в некоторой степени обладают признаками БД. Принято считать, что эта степень в большинстве случаев недостаточна (хотя могут быть исключения).

3.1. История

История возникновения и развития технологий баз данных может рассматриваться как в широком, так и в узком аспекте.

В широком смысле понятие истории баз данных обобщается до истории любых средств, с помощью которых человечество хранило и обрабатывало данные. Следует помнить, что недостатком этого подхода является размывание понятия «база данных» и фактическое его слияние с понятиями «архив» и даже «письменность».

История баз данных в узком смысле рассматривает базы данных в традиционном (современном) понимании. Эта история начинается с 1955 года, когда появилось программируемое оборудование обработки записей. Программное обеспечение этого времени поддерживало модель обработки записей на основе файлов. Для хранения данных использовались перфокарты.

Оперативные сетевые базы данных появились в середине 1960-х. Операции над оперативными базами данных обрабатывались в интерактивном режиме с помощью терминалов. Простые индексно-последовательные организации записей быстро развились к более мощной модели записей, ориентированной на наборы.

Следующий важный этап связан с появлением в начале 1970-х реляционной модели данных, благодаря работам Эдгара Кодда. Работы Кодда открыли путь к тесной связи прикладной технологии баз данных с математикой и логикой. За свой вклад в теорию и практику Эдгар Ф. Кодд также получил премию Тьюринга.

3.2. Виды баз данных

Классификация по модели данных. Примеры:

- Иерархическая.
- Объектная и объектно-ориентированная.
- Объектно-реляционная.
- Реляционная.
- Сетевая.
- Функциональная.

Иерархическая модель данных – это модель данных, где используется представление базы данных в виде древовидной (иерархической) структуры, состоящей из объектов (данных) различных уровней. Между объектами существуют связи, каждый объект может включать в себя несколько объектов более низкого уровня. Такие объекты находятся в отношении предка (объект более близкий к корню) к потомку (объект более низкого уровня), при этом возможна ситуация, когда объект-предок не имеет потомков или имеет их несколько, тогда как у объекта-потомка обязательно только один предок. Объекты, имеющие общего предка, называются близнецами (в программировании применительно к структуре данных дерево устоялось название братья). Базы данных с иерархической моделью одни из самых старых, и стали первыми системами управления базами данных для мейнфреймов. Разрабатывались в 1950-х и 1960-х, например, Information Management System (IMS) фирмы IBM

Объектные базы данных (также объектно-ориентированные системы управления базами данных) являются системой управления базами данных, в которых информация представлена в виде объектов, используется в объектно-ориентированном программировании. Объектные базы данных отличаются от реляционных баз данных, являющихся таблично-ориентированными. Объектно-реляционные базы данных являются гибридом обоих подходов. Объектные базы данных были рассмотрены в начале 1980-х годов.

Объектно-ориентированная база данных (ООБД) – база данных, в которой данные моделируются в виде объектов, их атрибутов, методов и классов.

Объектно-реляционная СУБД (ОРСУБД) – реляционная СУБД (РСУБД), поддерживающая некоторые технологии, реализующие объектно-ориентированный подход: объекты, классы и наследование реализованы в структуре баз данных и языке запросов.

Объектно-реляционными СУБД являются, например, широко известные Oracle Database, Informix, DB2, PostgreSQL.

Реляционная модель данных (РМД) – логическая модель данных, прикладная теория построения баз данных, которая является приложением к задачам обработки данных таких разделов математики, как теория множеств и логика первого порядка.

На реляционной модели данных строятся реляционные базы данных. Реляционная модель данных включает следующие компоненты:

- Структурный аспект (составляющая) – данные в базе данных представляют собой набор отношений.
- Аспект (составляющая) целостности – отношения (таблицы) отвечают определенным условиям целостности. РМД поддерживает декларативные ограничения целостности уровня домена (типа данных), уровня отношения и уровня базы данных.
- Аспект (составляющая) обработки (манипулирования) – РМД поддерживает операторы манипулирования отношениями (реляционная алгебра, реляционное исчисление).

Кроме того, в состав реляционной модели данных включают теорию нормализации.

Термин «реляционный» означает, что теория основана на математическом понятии отношение *(relation)*. В качестве неформального синонима термину «отношение» часто встречается слово таблица. Необходимо помнить, что «таблица» есть понятие нестрогое и неформальное и часто означает не «отношение» как абстрактное понятие, а визуальное представление отношения на бумаге или экране. Некорректное и нестрогое использование термина «таблица» вместо термина «отношение» нередко приводит к недопониманию. Наиболее частая ошибка состоит в рассуждениях о том, что РМД имеет дело с «плоскими», или «двумерными» таблицами, тогда как таковыми могут быть только визуальные представления таблиц. Отношения же являются абстракциями и не могут быть ни «плоскими», ни «неплоскими».

Для лучшего понимания РМД следует отметить три важных обстоятельства:

- модель является логической, то есть отношения являются логическими (абстрактными), а не физическими (хранимыми) структурами;

- для реляционных баз данных верен информационный принцип: всё информационное наполнение базы данных представлено одним и только одним способом – явным заданием значений атрибутов в кортежах отношений; в частности, нет никаких указателей (адресов), связывающих одно значение с другим;
- наличие реляционной алгебры позволяет реализовать декларативное программирование и декларативное описание ограничений целостности, в дополнение к навигационному (процедурному) программированию и процедурной проверке условий.

Принципы реляционной модели были сформулированы в 1969–1970 годах Э.Ф. Коддом (E.F. Codd). Идеи Кодда были впервые публично изложены в статье «A Relational Model of Data for Large Shared Data Banks», ставшей классической.

Строгое изложение теории реляционных баз данных (реляционной модели данных) в современном понимании можно найти в книге К.Дж. Дейта «Введение в системы баз данных» (C.J. Date. «An Introduction to Database Systems»).

Наиболее известными альтернативами реляционной модели являются иерархическая модель, и сетевая модель. Некоторые системы, использующие эти старые архитектуры, используются до сих пор. Кроме того, можно упомянуть об объектно-ориентированной модели, на которой строятся так называемые объектно-ориентированные СУБД, хотя однозначного и общепринятого определения такой модели нет.

Сетевая модель данных – логическая модель данных, являющаяся расширением иерархического подхода, строгая математическая теория, описывающая структурный аспект, аспект целостности и аспект обработки данных в сетевых базах данных. Разница между иерархической моделью данных и сетевой состоит в том, что в иерархических структурах запись-потомок должна иметь в точности одного предка, а в сетевой структуре данных у потомка может иметься любое число предков.

Сетевая БД состоит из набора экземпляров определенного типа записи и набора экземпляров определенного типа связей между этими записями.

Тип связи определяется для двух типов записи: предка и потомка. Экземпляр типа связи состоит из одного экземпляра типа записи предка и упорядоченного набора экземпляров типа записи потомка. Для данного типа связи L с типом записи предка P и типом записи потомка C должны выполняться следующие два условия:

- каждый экземпляр типа записи P является предком только в одном экземпляре типа связи L;
- каждый экземпляр типа записи C является потомком не более чем в одном экземпляре типа связи L.

Функциональные базы данных используются для решения аналитически задач, таких как финансовое моделирование и управление производительностью. Функциональная база данных или коротко функциональная модель отличается от реляционной модели. Функциональная модель также отличается от других аналогично названных концепций, включая модель функциональной базы данных DAPLEX и базы данных функциональных языков.

Функциональная модель является частью категории оперативной аналитической обработки (OLAP), поскольку она включает многомерное иерархическое объединение. Но она выходит за рамки OLAP, требуя ориентирования ячейки, подобно электронной таблице, где ячейки могут быть введены или рассчитаны как функции других ячеек. Также, как и в электронных таблицах, данная модель поддерживает интерактивные вычисления, в которых значения всех зависимых ячеек автоматически обновляются каждый раз, когда изменяется значение ячейки.

Классификация по среде постоянного хранения:

- Во вторичной памяти, или традиционная (англ. *conventional database*): средой постоянного хранения является периферийная энергонезависимая память (вторичная память) – как правило жёсткий диск. В оперативную

память СУБД помещает лишь кеш и данные для текущей обработки.

- В оперативной памяти (англ. *in-memory database, memory-resident database, main memory database*): все данные на стадии исполнения находятся в оперативной памяти.
- В третичной памяти (англ. *tertiary database*): средой постоянного хранения является отсоединяемое от сервера устройство массового хранения (третичная память), как правило на основе магнитных лент или оптических дисков.

Во вторичной памяти сервера хранится лишь каталог данных третичной памяти, файловый кеш и данные для текущей обработки; загрузка же самих данных требует специальной процедуры.

Классификация по содержимому

Примеры:

- Географическая.
- Историческая.
- Научная.
- Мультимедийная.
- Клиентская.

Мультимедиа (англ. *multimedia*) – контент, или содержимое, в котором одновременно представлена информация в различных формах – звук, анимированная компьютерная графика, видеоряд.

Например, в одном объекте-контейнере может содержаться текстовая, аудиальная, графическая и видеоинформация, а также, возможно, способ интерактивного взаимодействия с ней. Это достигается использованием определённого набора аппаратных и программных средств.

Термин *мультимедиа* также зачастую используется для обозначения носителей информации, позволяющих хранить значительные объемы данных и обеспечивать достаточно быстрый доступ к ним (первыми носителями такого типа были компакт-диски). В таком случае термин *мультимедиа* означает, что компьютер может использовать такие носители и предоставлять информацию пользователю через все возможные виды данных, такие как аудио, видео, анимация, изображение и другие в допол-

нение к традиционным способам предоставления информации, таким как текст.

Выделяют пять основных целей составления клиентской базы:

1) Сохранение и преемственность информации, которую решает данная база, это страховка от потери клиентов при увольнении менеджера по продажам или торгового представителя, а также быстрое вхождение в курс дела новых сотрудников.

2) Оценка перспективы. Данная БД ответит на вопрос о том, какой процент дистрибуции Вы имеете на рынке, какая доля клиентов лояльна, а какая еще не знает о Вашем предложении.

3) Аналитическая. Данная БД предполагает более глубокое представление информации о клиентах. Структура предприятия, персоналии, личные предпочтения, корзина покупки, периодичность заказа, сезонность и т.д. Вы получите возможность проводить различного рода анализ своих клиентов и строить прогнозы.

4) Маркетинговая. Если Ваша цель адресное воздействие на своих потенциальных клиентов и соответствующая экономия бюджета. Данная цель решается за счет:

а) правильного сегментирования своих клиентов,

б) глубокого изучения потребностей каждого сегмента,

в) подготовки индивидуального предложения для каждого сегмента,

г) проведения адресного воздействия.

5) Оценка смежных сегментов с целью расширения бизнеса. Клиенты редко интересуются чем-то узкоспециальным, а чаще имеют разносторонний спрос. Попытка сбора информации об интересах своих клиентов (дополнительных потребностей) позволяет осуществлять попутные продажи, или даже организовывать дополнительные направления бизнеса.

Классификация по степени распределения:

- Централизованная, или сосредоточенная (англ. *centralized database*): БД, полностью поддерживаемая на одном компьютере.
- Распределённая БД (англ. *distributed database*), составные части которой размещаются в различных узлах компьютерной сети в соответствии с каким-либо критерием:

a. неоднородная (англ. *heterogeneous distributed database*) – фрагменты распределённой БД в разных узлах сети поддерживаются средствами более одной СУБД;

b. однородная (англ. *homogeneous distributed database*) – фрагменты распределённой БД в разных узлах сети поддерживаются средствами одной и той же СУБД;

c. фрагментированная, или секционированная (англ. *partitioned database*) – методом распределения данных является фрагментирование (партиционирование, секционирование), вертикальное или горизонтальное;

d. тиражированная (англ. *replicated database*) – методом распределения данных является тиражирование (репликация).

Другие виды БД:

- пространственная (англ. *spatial database*) – БД, в которой поддерживаются пространственные свойства сущностей предметной области. Такие БД широко используются в геоинформационных системах;
- временная, или темпоральная (англ. *temporal database*) – БД, в которой поддерживается какой-либо *аспект времени*, не считая времени, определяемого пользователем;
- пространственно-временная (англ. *spatial-temporal database*) БД – БД, в которой одновременно поддерживается одно или более измерений в аспектах как пространства, так и времени;
- циклическая (англ. *round-robin database*) – БД, объём хранимых данных которой не меняется со временем, поскольку в процессе сохранения новых данных они заменяют более старые данные. Одни и те же ячейки для данных используются циклически.

3.3. Сверхбольшие базы данных

Сверхбольшая база данных (англ. *Very Large Database, VLDB*) – это база данных, которая занимает чрезвычайно большой объём на устройстве физического хранения. Термин подразумевает максимально возможные объёмы БД, которые опреде-

ляются последними достижениями в технологиях физического хранения данных и в технологиях программного оперирования данными.

Количественное определение понятия «чрезвычайно большой объём» меняется во времени. Так, в 1997 году самой большой в мире была текстовая база данных Knight Ridder's DIALOG объёмом 7 терабайт. В 2001 году самой большой считалась база данных объёмом 10,5 терабайт, в 2003 году – объёмом 25 терабайт. В 2005 году самыми крупными в мире считались базы данных с объёмом хранилища порядка сотни терабайт. В 2006 году поисковая машина Google использовала базу данных объёмом 850 терабайт.

К 2010 году считалось, что объём сверхбольшой базы данных должен измеряться по меньшей мере петабайтами.

К 2014 году по косвенным оценкам компания Google хранила на своих серверах до 10–15 эксабайт данных в совокупности.

По некоторым оценкам, к 2025 году генетики будут располагать данными о геномах от 100 миллионов до 2 миллиардов человек, и для хранения подобного объёма данных потребуется от 2 до 40 эксабайт.

Специалисты отмечают необходимость особых подходов к проектированию сверхбольших БД. Для их создания нередко выполняются специальные проекты с целью поиска таких системотехнических решений, которые позволили бы хоть как-то работать с такими большими объёмами данных. Как правило, необходимы специальные решения для дисковой подсистемы, специальные версии операционной среды и специальные механизмы обращения СУБД к данным.

Исследования в области хранения и обработки сверхбольших баз данных *VLDB* всегда находятся на острие теории и практики баз данных. В частности, с 1975 года проходит ежегодная конференция *International Conference on Very Large Data Bases* («Международная конференция по сверхбольшим базам данных»). Большинство исследований проводится под эгидой некоммерческой организации *VLDB Endowment* (Фонд целевого капитала «VLDB»), которая обеспечивает продвижение научных

работ и обмен информацией в области сверхбольших БД и смежных областях.

3.4. Система управления базами данных

Система управления базами данных (СУБД) – совокупность программных и лингвистических средств общего или специального назначения, обеспечивающих управление созданием и использованием баз данных.

Пошаговое руководство. Создание веб-страницы для отображения данных базы данных Access.

При помощи средства веб-разработки Microsoft Visual Web Developer можно создавать веб-страницы, которые работают с данными из различных источников, включая базы данных, XML-файлы и бизнес-объекты. В данном пошаговом руководстве показано, как работать с данными из базы данных программы Microsoft Access (MDB-файл).

Здесь вы узнаете, как выполняются следующие действия:

- Настройка разрешений для файлов MDB.
- Подключение к базе данных, содержащей элемент управления Access Data Source.
- Отображение данных из программы Access.

Базы данных Access имеют другую емкость и не настолько масштабируемы, как другие типы баз данных, например, базы данных Microsoft SQL Server. Обычно при создании веб-узла, поддерживающего только низкий трафик или ограниченное число пользователей, удобно использовать базу данных Access. Однако если веб-узел поддерживает большую нагрузку или большое количество пользователей, то лучше использовать базу данных SQL Server или другую базу данных, которая подходит для рабочих веб-узлов.

Обязательные компоненты

Для выполнения инструкций данного пошагового руководства необходимы следующие компоненты:

- Файл Northwind.mdb, содержащий Access-версию шаблонной базы данных Northwind.

- В ином случае можно использовать другой файл MDB из программы Access и подстраиваться под действия, производимые в данном пошаговом руководстве, чтобы используемые таблицы совпадали.
- Компоненты доступа к данным MDAC версии 2.7 или более поздней версии.

Если используется операционная система Microsoft Windows XP или Windows Server 2003, то компоненты доступа к данным MDAC версии 2.7 уже установлены. Однако если используется операционная система Microsoft Windows 2000, то необходимо обновить имеющуюся версию MDAC. Текущую версию MDAC можно загрузить с веб-узла Центра разработчиков доступа и хранения данных.

- Дополнительно, службы Microsoft Internet Information Services (IIS), установленные на локальном компьютере.

Это позволит вам проверять веб-узлы на наличие соответствующих прав на использование базы данных Access в рабочей среде.

Создание веб-узла и страницы

Если вы уже создали веб-узел в Visual Web Developer, выполнив Пошаговое руководство. Создание базовой веб-страницы в Visual Web Developer, то можно использовать этот веб-узел и перейти к следующему разделу. В противном случае создайте новый веб-узел и страницу, выполнив следующие действия.

Создание файлового веб-узла

1. Откройте Visual Web Developer.
2. В меню *Файл* выберите пункт *Создать веб-узел.*

Откроется диалоговое окно *Создать веб-узел.*

3. В группе *Установленные шаблоны Visual Studio* выберите *Веб-узел ASP.NET*.
4. В крайнем левом поле *Расположение* выберите *HTTP.*
5. Нажмите кнопку «Обзор».

Отобразится страница выбора расположения.

6. Щелкните *Local IIS* и нажмите *«Веб-узел по умолчанию»*.

7. Щелкните значок создания нового веб-приложения (), а затем назовите новое веб-приложение *AccessSample.*

8. Нажмите кнопку *Открыть.*

Появится диалоговое окно «Новый веб-узел», с расположением нового веб-приложения в крайнем правом поле Расположение.

9. В списке *Язык* выберите язык программирования, с которым вы предпочитаете работать.

Выбранный язык программирования будет языком по умолчанию для веб-узла, но можно задать язык программирования для каждой страницы отдельно.

10. Нажмите кнопку *ОК*.

Visual Web Developer создаст папку и новую страницу с именем Default.aspx. Веб-узел отобразится в *Обозревателе решений*.

3.5. Настройка разрешений для базы данных Access

Важным аспектом работы с MDB-файлами Access является правильная настройка разрешений. Если веб-приложение использует базу данных Access, то для доступа к данным у приложения должно быть разрешение на чтение MDB-файла. Кроме того, у такого приложения должно быть разрешение на запись / в папке, содержащей MDB-файл. Разрешение на запись необходимо потому, что программа Access создает дополнительный файл с расширением LDB, в котором она хранит информацию о блокировках базы данных для текущих пользователей. LDB-файл создается во время выполнения.

По умолчанию веб-приложения ASP.NET работают в контексте локальной учетной записи на компьютере с именем ASPNET (для операционных систем Windows 2000 и Windows XP) или в контексте учетной записи NETWORK SERVICE (для Windows Server 2003). Например, для операционных систем Windows 2000 и Windows XP Professional, если веб-сервер называется ABCServer, приложения ASP.NET на компьютере ABCServer выполняются в контексте локальной учетной записи ABCServer\ ASPNET. Поэтому для использования базы данных Access в веб-приложении ASP.NET нужно настроить папку, содержа-

щую базу данных Access, чтобы она имела разрешения на чтение и запись для локальной учетной записи пользователя ASPNET.

При создании веб-узла в Visual Web Developer программа Visual Web Developer создает внутри текущего корневого каталога папку с именем App_Data. Эта папка должна служить хранилищем для данных приложения, в том числе баз данных Access. Кроме того, папка App_Data используется ASP.NET для хранения баз данных, поддерживаемых системой, например, базы данных членства и ролей. При создании папки App_Data средством Visual Web Developer учетной записи пользователя ASPNET или NETWORK SERVICE предоставляются права на чтение и запись в этой папке.

В данной части пошагового руководства будут проверяться разрешения папки App_Data, чтобы удостовериться в том, что она будет работать правильно при запуске приложения.

Установка разрешений в папке App_Data

1. В проводнике Windows перейдите к корневой папке веб-узла. Расположением по умолчанию нового веб-узла является c:\inetpub\wwwroot\AccessSample.

2. Если папка *App_Data* не существует, то ее надо создать. По умолчанию Visual Web Developer создает эту папку при создании нового веб-узла.

3. Щелкните правой кнопкой мыши папку App_Data, щелкните *Свойства* и нажмите вкладку *Безопасность* (рисунок 3.2).

4. В списке *Имена пользователей* или групп найдите любую из этих учетных записей пользователя:

- если на компьютере установлена операционная система Windows XP Professional или Windows 2000, то ищите учетную запись *computer*\ASPNET;
- если на компьютере установлена операционная система Windows Server 2003, то ищите учетную запись NETWORK SERVICE.

5. Проверьте, имеет ли учетная запись разрешения на запись и чтение для папки App_Data.

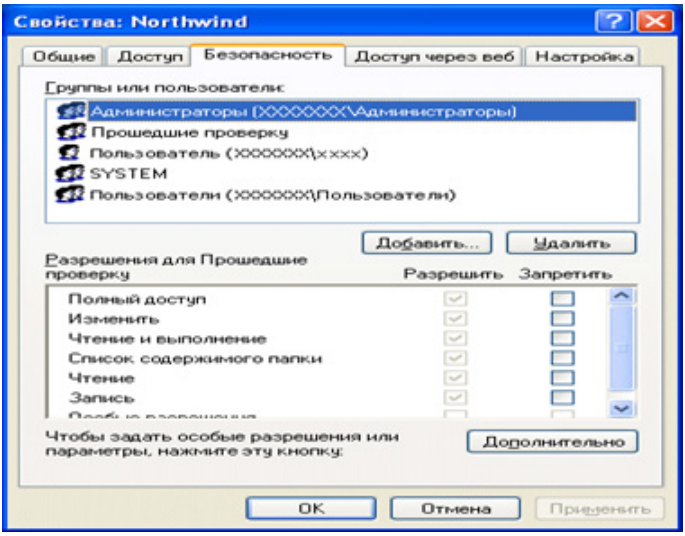


Рисунок 3.2 – Вкладка «Безопасность»

Использование данных из программы Access на веб-странице ASP.NET

Теперь можно использовать базу данных Access в веб-странице. Будет использоваться элемент управления AccessDataSource.

Добавление элемента управления Access Data Source на страницу

1. В Visual Web Developer, в *Обозревателе* решений щелкните правой кнопкой мыши папку App_Data, а затем выберите «Добавить существующий элемент».
2. Найдите файл Northwind.mdb (или другой MDB-файл программы Access), который будет использован в ходе данного пошагового руководства.
3. В папке App_Data щелкните MDB-файл и нажмите кнопку «Добавить». MDB-файл добавится в приложение.
4. Откройте страницу Default.aspx и переключитесь в режим конструктора.
5. Из группы «Данные» в «Панели элементов» перетащите на страницу элемент управления AccessDataSource.

Если контекстное меню *Задачи Access Data Source* не отображается, то щелкните правой кнопкой мыши элемент управления AccessDataSource и нажмите кнопку *Показать смарт-тег*.

6. В контекстном меню *Задачи Access Data Source* выберите команду *Настройка источника данных.*

Появится мастер *«Настройки источника данных» – <DataSourceName>*.

7. На странице *Выбор базы данных* в поле *Файл данных Microsoft Access* введите *~/App_Data/Northwind.mdb*.

В ином случае нажмите кнопку *Обзор* и в диалоговом окне *Выбор базы данных Microsoft Access* переместите файл Northwind.mdb в папку App_Data.

8. Нажмите кнопку Далее.

Отобразится страница *Настройка инструкции Select.*

9. Щелкните *Укажите столбцы из таблицы или представления.*

10. В списке «Имя» щелкните *Категории.*

11. Отметьте флажки *CategoryID, CategoryName и Description.*

12. Нажмите кнопку *Далее.*

Отобразится страница *Проверка запроса.*

Если необходимо проверить запрос, то щелкните *Проверка запроса.*

13. Нажмите кнопку *Готово.*

14. В *Панели элементов* из группы «Данные» перетащите на страницу элемент управления GridView.

Если контекстное меню *Задачи GridView* не отображается, щелкните правой кнопкой мыши элемент управления GridView и нажмите кнопку Показать смарт-тег.

15. В меню *Задачи GridView* в поле *Выбор источника данных* выберите *AccessDataSource1*.

Проверка страницы

Теперь можно проверить работу страницы. Чтобы запустить страницу, нажмите клавиши CTRL + F5.

Все строки данных из таблицы категорий отображаются в элементе управления GridView.

Следующие действия

Данное пошаговое руководство рассказывает о базовых действиях, которые необходимо совершать при работе с данными из программы Access на веб-странице ASP.NET. Модель привязки данных ASP.NET позволяет работать с данными из различных источников одним способом. Например, доступны следующие действия:

- Использование элементов управления для фильтрования данных, отображаемых на странице. Подробные сведения см. в разделе Пошаговое руководство. Основы доступа к данным на веб-страницах.
- Обновление, вставка и удаление данных из базы данных Access. Подробные сведения см. в разделе Пошаговое руководство. Редактирование и вставка данных в веб-страницы с помощью серверного веб-элемента управления DetailsView
- Создание страниц для отображения данных из таблиц Access, которые имеют отношения «основной/подробности». Подробные сведения см. в разделе Пошаговое руководство: создание основных веб-страниц и страниц подробностей в Visual Studio.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1. Дайте определение понятиям: «информация», «информационная безопасность», «защита информации», «информационная угроза».
2. Дайте характеристику основным составляющим информационной безопасности.
3. Перечислите основные объекты защиты.
4. Дайте характеристику понятиям «государственная тайна», «конфиденциальная информация» и «персональные данные».
5. Дайте характеристику средствам защиты информации.
6. Необходимость обеспечения безопасности в информационных системах.
7. Прогресс информационных технологий и информационная безопасность.
8. Нормативно-правовые аспекты информационной безопасности.
9. Классификация угроз безопасности информационных объектов.
10. Основные виды каналов утечки информации.
11. Умышленные и неумышленные угрозы информационной безопасности.
12. Внешние угрозы информационной безопасности.
13. Мотивы и цели компьютерных преступлений.
14. Статьи уголовного кодекса о компьютерных преступлениях.
15. Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение.
16. Объекты информационной безопасности на предприятии.
17. Организационные методы обеспечения информационной безопасности.
18. Физическая защита информационных систем.
19. Программно-технические методы обеспечения информационной безопасности.

20. Идентификация и аутентификация.
21. Государственное регулирование информационной безопасности в Кыргызстане.
22. Несанкционированный доступ и защита от него.
23. Проблема информационной безопасности в историческом аспекте.
24. Предупреждение компьютерных преступлений.
25. Способы воздействия угроз на информационный объект.
26. Признаки воздействия вирусов на компьютерную систему.
27. Фрагментарный и системный подходы к защите информации.
28. Причины и условия, способствующие совершению компьютерных преступлений.
29. Меры предупреждения преступлений в сфере компьютерной информации.
30. История вредоносных программ.
31. Защита учетной информации коммерческих фирм.
32. Свойства экономической информации, нарушаемые при несанкционированном доступе.
33. Исторические аспекты компьютерных преступлений.
34. Экономическая информация как объект безопасности.
35. Перечень сведений, которые не могут составлять коммерческую тайну.
36. Стратегия злоумышленника при несанкционированном доступе.
37. Структура службы безопасности компании.
38. Теоретические аспекты информационной.
39. Основные понятия информационной.
40. Понятия информационных угроз и их виды.
41. Компьютерные преступления и наказания.
42. Принципы построения системы информационной безопасности.
43. Подходы, принципы, методы и средства обеспечения безопасности.
44. Организационно-техническое обеспечение компьютерной безопасности.

45. Электронная цифровая подпись и особенности ее применения.
46. Защита информации в Интернете.
47. Организация системы защиты информации экономических систем.
48. Этапы построения системы защиты информации.
49. Политика безопасности.
50. Оценка эффективности инвестиций в информационную безопасность.
51. Обеспечение компьютерной безопасности учетной информации.
52. Сущность криптографических методов.
53. Организационно-административные мероприятия обеспечения компьютерной безопасности.
54. Организация конфиденциального делопроизводства.
55. Принципы обеспечения информационную безопасности на основе инженерно-технического обеспечения.
56. Типы и субъекты информационных угроз.
57. Базы данных. Основные определения.
58. СУБД. Функции СУБД.
59. Реляционная модель данных.
60. Этапы разработки базы данных.
61. Нормализация данных.
62. Целостность данных. Внешние ключи.
63. Транзакции. Блокировки.
64. Операторы управления потоком данных.
65. Виды угроз ИС. Методы защиты данных.
66. Управление учетными записями пользователей.
67. Средства резервного копирования данных.
68. Понятие Access.
69. Использование данных из программы Access.

ТЕМЫ ДЛЯ РЕФЕРАТОВ

1. Сущность организационной защиты информации и ее место в комплексной системе защиты информации.
2. Методы и формы организационной защиты информации.
3. Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации.
4. Определение категорий сотрудников и подбор персонала для работы с конфиденциальной информацией.
5. Оформление допуска сотрудников к конфиденциальной информации.
6. Текущая работа с персоналом и обучение сотрудников правилам и приёмам работы с конфиденциальной информацией.
7. Организация разрешительной системы доступа к конфиденциальной информации.
8. Организация физической охраны предприятия.
9. Организация пропускного и внутри объектного режимов.
10. Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями.
11. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.
12. Организация защиты информации при приёме в организации посетителей.
13. Организация защиты конфиденциальной информации при осуществлении международного сотрудничества.
14. Организация защиты информации при осуществлении рекламной и выставочной деятельности.
15. Организация защиты информации при подготовке материалов к открытому опубликованию.
16. Аналитическая работа как основа управления системой организационной защиты информации.
17. Организационная защита конфиденциальной продукции в процессе её изготовления, хранения и транспортировки.
18. Ответственность по факту разглашения или утраты документов, содержащих конфиденциальную информацию.

19. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
20. История развития, назначение и роль баз данных.
21. Файловые системы и базы данных.
22. Структуры данных и базы данных.
23. Способы хранения информации в базах данных.
24. Способы повышения эффективности обработки данных за счет их организации.
25. Общая характеристика, назначение, возможности, состав и архитектура СУБД.
26. Классификация СУБД.
27. Информационное, лингвистическое, математическое, аппаратное, организационное, правовое обеспечения СУБД.
28. Типология баз данных. Документальные базы данных. Фактографические базы данных.
29. Типология баз данных. Гипертекстовые и мультимедийные базы данных.
30. Типология баз данных. Объектно-ориентированные базы данных.
31. Типология баз данных. Распределенные базы данных. Коммерческие базы данных.
32. Недостатки реляционных СУБД.
33. Объектные расширения реляционных СУБД.
34. Средства автоматизации проектирования баз данных.
35. Централизация логики приложения на сервере базы данных.
36. Информационные хранилища. OLAP-технология. XML-серверы.
37. Принципы построения БД. Управление складами данных.
38. Проблема создания и сжатия больших информационных массивов, информационных хранилищ и складов данных.
39. Фрактальные методы в архивации. Серверы баз данных.
40. Средства поддержания целостности базы данных.
41. СУБД, ориентированные на конкретные платформы. СУБД Access в Microsoft Windows.

42. Базы данных реального времени. Защита информации в СУБД.
43. Жизненный цикл базы данных.
44. Циклическая база данных.
45. Сжатие без потерь в реляционных СУБД.
46. Хранение деревьев в реляционных базах данных.
47. Способы переноса данных с одного типа БД в другую. На примере переноса данных из MySQL в Access.
48. Способы переноса данных с одного типа БД в другую. На примере переноса данных из Access в MySQL.
49. Экспорт/импорт между базами данных различных производителей.
50. Реальные и фантастические разработки БД.
51. Физическое хранение реляционных таблиц.
52. Сериализация транзакций в БД.
53. Анализ качества баз данных.
54. Пути формирования баз данных для директ-маркетинга.
55. Архитектура и функционирование адресных баз данных.
56. Сверхбольшие базы данных.
57. Эксплуатация баз данных. Состав, порядок планирования и проведения регламентных работ.
58. Эксплуатация баз данных. Сервисные средства СУБД.
59. Эксплуатация баз данных. Задачи администратора базы данных.
60. Эксплуатация баз данных. Организация труда обслуживающего персонала.

ТЕСТЫ ДЛЯ КОНТРОЛЯ ЗНАНИЙ

1. Под информационной безопасностью понимается…

а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре;

б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия;

в) нет правильного ответа.

2. Защита информации – это…

а) комплекс мероприятий, направленных на обеспечение информационной безопасности;

б) процесс разработки структуры базы данных в соответствии с требованиями пользователей;

в) небольшая программа для выполнения определенной задачи.

3. От чего зависит информационная безопасность?

а) от компьютеров;

б) от поддерживающей инфраструктуры;

в) от информации.

4. Основные составляющие информационной безопасности:

а) целостность;

б) достоверность;

в) конфиденциальность.

5. Доступность – это…

а) возможность за приемлемое время получить требуемую информационную услугу;

б) логическая независимость;

в) нет правильного ответа.

6. Целостность – это...

а) целостность информации;

б) непротиворечивость информации;

в) защищенность от разрушения.

7. Конфиденциальность – это...

а) защита от несанкционированного доступа к информации;

б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов;

в) описание процедур.

8. Для чего создаются информационные системы?

а) получения определенных информационных услуг;

б) обработки информации;

в) все ответы правильные.

9. Целостность можно подразделить:

а) статическую;

б) динамичную;

в) структурную.

10. Где применяются средства контроля динамической целостности?

а) анализе потока финансовых сообщений;

б) обработке данных;

в) при выявлении кражи, дублирования отдельных сообщений.

11. Какие трудности возникают в информационных системах при конфиденциальности?

а) сведения о технических каналах утечки информации являются закрытыми;

б) на пути пользовательской криптографии стоят многочисленные технические проблемы;

в) все ответы правильные.

12. Угроза – это…

а) потенциальная возможность определенным образом нарушить информационную безопасность;

б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;

в) процесс определения отвечает на текущее состояние разработки требованиям данного этапа.

13. Атака – это…

а) попытка реализации угрозы;

б) потенциальная возможность определенным образом нарушить информационную безопасность;

в) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это...

а) потенциальный злоумышленник;

б) злоумышленник;

в) нет правильного ответа.

15. Окно опасности – это…

а) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется;

б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области;

в) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере.

16. Кто является основным ответственным за определение уровня классификации информации?

а) руководитель среднего звена;

б) высшее руководство;

в) владелец;

г) пользователь.

17. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) сотрудники;

б) хакеры;

в) атакующие;

г) контрагенты (лица, работающие по договору).

18. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

а) снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования;

б) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации;

в) улучшить контроль за безопасностью этой информации;

г) снизить уровень классификации этой информации.

19. Что самое главное должно продумать руководство при классификации данных?

а) типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным;

б) необходимый уровень доступности, целостности и конфиденциальности;

в) оценить уровень риска и отменить контрмеры;

г) управление доступом, которое должно защищать данные.

20. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) владельцы данных;

б) пользователи;

в) администраторы;

г) руководство.

21. Что такое процедура?

а) правила использования программного и аппаратного обеспечения в компании;

б) пошаговая инструкция по выполнению задачи;

в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах;

г) обязательные действия.

22. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

а) поддержка высшего руководства;

б) эффективные защитные меры и методы их внедрения;

в) актуальные и адекватные политики и процедуры безопасности;

г) проведение тренингов по безопасности для всех сотрудников.

23. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

а) никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски;

б) когда риски не могут быть приняты во внимание по политическим соображениям;

в) когда необходимые защитные меры слишком сложны;

г) когда стоимость контрмер превышает ценность актива и потенциальные потери.

24. Что такое политики безопасности?

а) пошаговые инструкции по выполнению задач безопасности;

б) общие руководящие требования по достижению определенного уровня безопасности;

в) широкие, высокоуровневые заявления руководства;

г) детализированные документы по обработке инцидентов безопасности.

25. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) анализ рисков;

б) анализ затрат / выгоды;

в) результаты ALE;

г) выявление уязвимостей и угроз, являющихся причиной риска.

26. База данных – это…

а) специальным образом организованная и хранящаяся на внешнем носителе совокупность взаимосвязанных данных о некотором объекте;

б) произвольный набор информации;

в) совокупность программ для хранения и обработки больших массивов информации;

г) интерфейс, поддерживающий наполнение и манипулирование данными;

д) компьютерная программа, позволяющая в некоторой предметной области делать выводы, сопоставимые с выводами человека-эксперта.

27. В записи файла реляционной базы данных (БД) может содержаться:

а) исключительно однородная информация (данные только одного типа);

б) только текстовая информация;

в) неоднородная информация (данные разных типов);

г) только логические величин;

д) исключительно числовая информация.

28. Предположим, что некоторая база данных содержит поля *ФАМИЛИЯ, ГОД РОЖДЕНИЯ, ДОХОД***. При поиске по условию** *ГОД РОЖДЕНИЯ > 1958 AND ДОХОД < 3500* **будут найдены фамилии лиц:**

а) имеющих доход не менее 3500, и старше тех, кто родился в 1958 году;

б) имеющих доход менее 3500, или тех, кто родился е 1958 году и позже;

в) имеющих доход менее 3500, и родившихся в 1958 году и позже;

г) имеющих доход менее 3500, и родившихся в 1959 году и позже;

д) имеющих доход менее 3500, и тех, кто родился в 1958 году.

29. Какой из вариантов не является функцией СУБД?

а) реализация языков определения и манипулирования данными;

б) обеспечение пользователя языковыми средствами манипулирования данными;

в) поддержка моделей пользователя;

г) защита и целостность данных;

д) координация проектирования, реализации и ведения БД.

30. Система управления базами данных представляет собой программный продукт, входящий в состав:

а) прикладного программного обеспечения;

б) операционной системы;

в) уникального программного обеспечения;

г) системного программного обеспечения;

д) систем программирования.

31. Какая наименьшая единица хранения данных в БД?

а) хранимое поле;

б) хранимый файл;

в) ничего из вышеперечисленного;

г) хранимая запись;

д) хранимый байт.

32. Что обязательно должно входить в СУБД?

а) процессор языка запросов;

б) командный интерфейс;

в) визуальная оболочка;

г) система помощи.

33. Перечислите преимущества централизованного подхода к хранению и управлению данными:

а) возможность общего доступа к данным;

б) поддержка целостности данных;

в) соглашение избыточности;

г) сокращение противоречивости.

34. Предположим, что некоторая база данных описывается следующим перечнем записей:

а) Иванов, 1956, 2400;

б) Сидоров, 1957, 5300;

в) Петров, 1956, 3600;

г) Козлов, 1952, 1200.

35. Какие из записей этой БД поменяются местами при сортировке по возрастанию, произведенной по первому полю:

а) 3 и 4;

б) 2 и 3;

в) 2 и 4;

г) 1 и 4;

д) 1 и 3.

36. Структура файла реляционной базы данных (БД) меняется:

а) при изменении любой записи;

б) при уничтожении всех записей;

в) при удалении любого поля;

г) при добавлении одной или нескольких записей;

д) при удалении диапазона записей.

37. Как называется набор хранимых записей одного типа?

а) хранимый файл;

б) представление базы данных;

в) ничего из вышеперечисленного;

г) логическая таблица базы данных;

д) физическая таблица базы данных.

38. Таблица СУБД содержит:

а) информацию о совокупности однотипных объектов;

б) информацию о совокупности всех объектов, относящихся к некоторой предметной области;

в) информацию о конкретном объекте.

39. Строки таблицы СУБД содержат:

а) информацию о совокупности однотипных объектов;

б) информацию о совокупности всех объектов, относящихся к некоторой предметной области;

в) информацию о конкретном объекте.

40. Столбцы таблицы СУБД содержат:

а) информацию о совокупности однотипных объектов;

б) информацию о совокупности всех объектов, относящихся к некоторой предметной области;

в) совокупность значений одного из атрибутов для всех однотипных объектов.

41. Структура таблицы СУБД определяется:

а) размерностью таблицы;

б) списком наименований столбцов таблицы;

в) списком наименований столбцов и номеров строк таблицы.

42. Поле данных в СУБД – это…

а) значение атрибута для конкретного объекта;

б) элемент структуры таблицы;

в) список значений атрибута для всех однотипных объектов.

43. Ключевое поле таблицы в СУБД – это…

а) строку таблицы, содержащей уникальную информацию;

б) совокупность полей таблицы, которые однозначно определяют каждую строку;

в) столбец таблицы, содержащей уникальную информацию.

44. Таблица в СУБД может иметь:

а) только одно ключевое поле;

б) только два ключевых поля;

в) любое количество ключевых полей.

45. В текстовом поле СУБД MS Access можно хранить:

а) только буквенную (символьную) информацию;

б) маску ввода;

в) картинки.

46. Мастер подстановок в СУБД MS Access используется:

а) для создания новых полей;

б) для придания значений полей из других таблиц, или введение фиксированного списка данных;

в) для расчета функций.

47. В режиме конструктора таблицы СУБД Access можно:

а) добавить новое поле;

б) набрать текстовый документ;

в) выполнить вычисления.

48. Изменить формат числового поля в СУБД Access можно:

а) набрав соответствующую комбинацию клавиш;

б) в конструкторе таблицы;

в) изменив название поля в самой таблице.

49. Имя поля таблицы в СУБД Access может хранить:

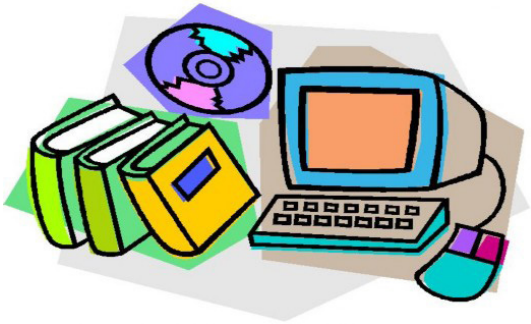
а) до 64-х символов;

б) только знаки 0 и 1;

в) нет ограничений на количество символов.

50. Для каких целей удобно использовать запросы в MS Access? Выберите наиболее правильное и полное толкование:

а) с их помощью можно просматривать, анализировать и изменять данные из нескольких таблиц и других запросов. Они также используются как источник для форм и отчетов;
б) с их помощью можно просматривать, анализировать и изменять данные из нескольких таблиц, запросов, отчетов, форм. Они используются в качестве источника данных для таблиц и отчетов;
в) с их помощью можно просматривать, анализировать и изменять данные из нескольких таблиц, отчетов, форм.



ГЛОССАРИЙ

Аналитическая работа – комплексное исследование различной целевой направленности, предназначенное для выявления, структуризации и изучения опасных объективных и субъективных, потенциальных и реальных ситуаций, которые могут создать риск для экономической безопасности фирмы, ее деятельности или персонала, привести к материальным, финансовым или иным убыткам, падению престижа фирмы или ее продукции.

Аналитическая работа по выявлению каналов несанкционированного доступа к конфиденциальной информации – прогнозирование и выявление на основе комплексного исследования сложившихся или предполагаемых ситуаций состава и особенностей образования *каналов несанкционированного доступа* к конфиденциальной информации конкретной фирмы в единстве с изучением характера возможных *угроз* ее *информационной безопасности.*

Аналитическая работа с источником конфиденциальной информации – комплексное исследование максимального числа источников, владеющих или содержащих конфиденциальные сведения.

Аналитическая работа с источником угрозы конфиденциальной информации – комплексное исследование максимального числа объектов и субъектов, представляющих опасность для Информационной безопасности фирмы.

Аналитическая работа с каналом объективного распространения конфиденциальной информации – комплексное исследование максимального числа коммуникативных каналов, по которым перемещаются конфиденциальные сведения в санкционированном режиме.

Аппаратный сервер – узкоспециализированное решение со встроенным программным обеспечением в ПЗУ (англ. *firmware*; в отличие от компьютеров, где программное обеспечение необходимо устанавливать), определяющим специализацию и возможные предоставляемые услуги.

Аутентичность информации – избежание недостатка полноты или точности информации при ее санкционированных изменениях.

База данных (БД) (Database; Data base (DB) (фр. *Base de donnees*)) – совокупность связанных данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования, независимая от прикладных программ.

Безопасность (Safety; Security) – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, точнее, безопасность – это защищенность жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, состояние, при котором чему-либо или кому-либо не угрожает опасность.

Безопасность сети (Network security) – меры, предохраняющие информационную сеть:

от несанкционированного доступа; от случайного или преднамеренного вмешательства в нормальные действия или от попыток разрушения ее компонентов. Безопасность информационной сети включает защиту оборудования, программного обеспечения, данных и персонала.

Безопасность информационная – составная *часть экономической безопасности* предпринимательской деятельности.

Безопасность информационных ресурсов (информации) – защищенность информации во времени и пространстве от любых объективных и субъективных *угроз (опасностей)*, возникающих в обычных условиях функционирования фирмы и *условиях экстремальных ситуаций*. Безопасность ценной документированной информации (документов) определяется уровнем ее защищенности от стихийных бедствий, других неуправляемых событий, пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу *несанкционированного доступа* к документам, делам, базам данных, а также опасностей неправомерного использования кем-либо ценных сведений, нарушения их сохранности, целостности конфиденциальности.

Безопасность предполагает также защищенность конфиденциальной информации *в информационных системах* от случайных и преднамеренных воздействий естественного и искусственного свойства, направленных на изменение степени доступности ценных сведений в машинной и вне машинных сфер.

Безопасность маркетинговая – составная *часть экономической безопасности* предпринимательской деятельности.

Безопасность правовая – составная *часть экономической безопасности* предпринимательской деятельности.

Безопасность физическая – составная *часть экономической безопасности* предпринимательской деятельности.

Безопасность экономическая – всесторонняя защищенность предпринимательской деятельности, деловых интересов каждого творческого коллектива, предприятия, фирмы и предпринимателя в большом и малом бизнесе во времени и пространстве.

Владелец информационных ресурсов – субъект, осуществляющий владение и пользование указанным объектом и реализующий полномочия распоряжения в пределах, установленных законом и собственникам *информационных ресурсов.*

Видеограмма – изображение электронного документа на экране дисплея. В полном смысле слова документом не является, представляет собой заверенную или незаверенную копию документа (как и факсограмма).

Виртуальный сервер, локальный сервер – комплект программного обеспечения, обеспечивающий разработку сетевых программ в режиме клиент-сервер локально на одном компьютере без необходимости доступа к сети.

Данные Data – сведения, полученные путем измерения, наблюдения, логических или арифметических операций и представленные в форме, пригодной для постоянного хранения, передачи и (автоматизированной) обработки.

Документ выделенного хранения – ценный документ, изъятый по какой-то причине из дела, оформленный в самостоятельное дело и переведенный на *инвентарный вид учета*.

Документ конфиденциальный – документ ограниченного доступа, на любом носителе, содержащий информацию, отража-

ющую приоритетные достижения в сфере экономической, производственной, предпринимательской, управленческой и другой деятельности, а также информацию, состав которой является принадлежностью служебной деятельности.

Документ машиночитаемый – официальный документ, созданный дня обеспечения работы вычислительной техники.

Документ подлинный – документ, сведения об авторе, времени и месте создания которого, содержащиеся в самом докуете или выявленные иным путем, подтверждают достоверность его происхождения.

Документ секретный – документ на любом носителе, отнесенный *к информационным ресурсам ограниченного доступа* и содержащий сведения, составляющие *государственную тайну*, которые включены в утвержденный специальный *перечень таких сведений*.

Документ черновой – рукописный, машинописный или электронный документ, отражающий работу автора или редактора над его текстом.

Документирование – запись информации на различных носителях по установленным правилам.

Документирование конфиденциальной информации – этап стадии *исполнения конфиденциального документа*.

Документооборот – движение документов в организации с момента их создания или получения до завершения исполнения или отправки.

Документооборот (документопоток) защищенный – контролируемое движение *конфиденциальной документированной информации* по регламентированным пунктам приема, обработки, рассмотрения, исполнения, использования и хранения в жестких условиях организационного и технологического обеспечения безопасности *как носителя информации*, так и самой информации.

Документопоток – движение документов в определенном направлении для облегчения решения управленческих задач. Существует: входящий (входной), исходящий (выходной) и внутренний документопотоки.

Допуск к конфиденциальной информации – *часть разрешительной (разграничительной) системы доступа персонала к конфиденциальной информации*, представляет собой процедуру оформления права сотрудника фирмы или иного лица на *доступ к информации* ограниченного распространения и одновременно правовой акт согласия (разрешения) *собственника* или *владельца* информации на передачу ее для работы конкретному лицу.

Доступ к информации несанкционированный – случайное или преднамеренное овладение конфиденциальными сведениями и возможное опасное воздействие на них лиц, не имеющих права доступа к конкретной *защищаемой информации.* Доступ, не санкционированный полномочным должностным лицом, считается незаконным.

Доступ к информации санкционированный – *часть разрешительной (разграничительной) системы доступа персонала к конфиденциальной информации*, представляет собой практическую реализацию права сотрудника на работу с подобной информацией, необходимой ему для выполнения возложенных на него функций. Доступ санкционируется полномочным должностным лицом (первым руководителем, его заместителем, руководителем подразделения, службы или направления деятельности) в отношении конкретной информации и конкретного сотрудника фирмы.

Доступ к компьютеру – санкционирование полномочным должностным лицом работы сотрудника с определенным составом вычислительной техники.

Доступ к базам данным и файлам – санкционирование полномочным должностным лицом работы сотрудника с определенным составом конфиденциальных сведений и файлов.

Доступ к машинным носителям, находящимся вне ЭВМ – санкционирование полномочным должностным лицом работы сотрудника с определенным составом носителей информации.

Достоверность информации – в криптографии: общая точность и полнота информации. Достоверность информации обратно пропорциональна вероятности возникновения ошибок в информационной системе.

Доступность информации – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Защита информации – совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера.

Защита информации в службе персонала – направление обеспечения *безопасности информации* фирмы в части сохранения *конфиденциальности* персональных данных, которые формируются в процессе документирования трудовых правоотношений сотрудников с фирмой.

Защита информации при ведении переговоров и совещаний – направление обеспечения *безопасности информации*, которое распространяется в процессе этих мероприятий.

Защищенность информационной системы Security – способность системы противостоять несанкционированному доступу к конфиденциальной информации, ее искажению или разрушению.

Злоумышленник Intruder – субъект, оказывающий на информационный процесс воздействия с целью вызвать его отклонение от условий нормального протекания. В криптографии считается, что в распоряжении злоумышленника имеются все необходимые для выполнения его задачи технические средства, созданные на данный момент. Злоумышленник – лицо (группа лиц), предполагающее совершить или умышленно совершающее противоправные действия с целью овладения информацией, составляющей тот или иной *вид тайны*.

Единица хранения архивных документов – учетная и классификационная единица, представляющая собой физически обособленный документ или совокупность документов, имеющих самостоятельное значение.

Идентификатор – персональное обозначение (код, шифр, имя, пропуск, персональная карточка определенного цвета с фотографией, магнитная или иная карта и т. п.), позволяющее однозначно выделить идентифицируемый объект среди других в полном множестве объектов. Используется в системах доступа.

Идентификация пользователя – отождествление лиц по их характеристикам или путем опознавания по приметам или документам в целях определение полномочий, связанных с *доступом к конфиденциальной информации*. Присвоение имени пользователю информационной системы, потребителю информации.

Инженерно-технический элемент системы защиты информации – комплекс организационно-технических, технических и технологических мероприятий защиты информации, предназначенных для пассивного и активного *противодействия* средствам технической разведки и формирования *рубежей охраны территории, здания, помещений и оборудования* с помощью совокупности *технических средств*.

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информационные ресурсы ограниченного доступа – документы и массивы документов, содержащие сведения, отнесенные к тому или иному виду *тонны* и подлежащие защите, охране, наблюдению и контролю.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информация защищаемая – синоним понятий *информация секретная и информация конфиденциальная*. Информация может быть отнесена к категории защищаемой, если ее содержание неизвестно конкуренту или противнику, а также, если указанная неизвестность дает определенные преимущества в политической, экономической или предпринимательской деятельности. При отнесении информации к защищаемой должны соблюдаться принципы законности, обоснованности, своевременности и др.

Информация конфиденциальная – документированная информация, относимая к одному из видов *негосударственной тайны* или *персональным данным*, доступ к которой ограничивается в соответствии с законами. Решение о таком ограничении принимает *собственник* или владелец указанной информации,

т. е. он устанавливает правовой режим информации, являющейся *его интеллектуальной собственностью* (*кроме* персональных данных).

Информация ценная – информация, которая составляет *интеллектуальную собственность* предпринимателя или группы предпринимателей и дает им возможность производить качественную продукцию, товары и услуги, пользующиеся повышенным спросом на рынке, заключать выгодные сделки, находить новых клиентов, покупателей как самой продукции, так и технологии ее производства.

Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Источник конфиденциальной информации – объективно пассивный накопитель (концентратор) *конфиденциальной информации*. В научной литературе часто используется альтернативный для сферы защиты информации термин – «носитель конфиденциальной информации» по аналогии с термином «секретоноситель».

Источник угрозы конфиденциальной информации – объективные и субъективные явления, события, факторы, действия и обстоятельства, содержащие опасность для *ценной информации*. К объективным источникам можно отнести: *экстремальные ситуации*, несовершенство технических средств и др. Субъективные источники связаны с человеческим фактором и включают *злоумышленников* различного рода, *посторонних лиц*, посетителей, неквалифицированный или безответственный персонал, психически неполноценных людей, сотрудников, обиженных руководством фирмы, и др.

Канал несанкционированного доступа к информации – совокупность незащищенных или слабо защищенных фирмой направлений возможной *утраты конфиденциальной информации*, *которые злоумышленник* использует для получения необходимых сведений, преднамеренного незаконного доступа *к защищаемой информации.*

Клиент – активное и отдельное от сервера программное обеспечение, использующее данные, поставляемые сервером путем передачи клиентских запросов серверу.

Web-клиент – как программа – браузер. Web-клиент как устройство – устройство, основным приложением которого (с точки зрения разработчика устройства или маркетолога) является браузер.

Конвертование (пакетирование) конфиденциальных документов – совокупность технических приемов, предотвращающих несанкционированное тайное вскрытие конвертов (пакетов) и извлечение из них конфиденциальных документов, а также прочтение текста без извлечения документа и даже вскрытия конверта.

Контроль доступа – регулярные проверочные действия по определению правомерности разрешений на доступ и доступа сотрудников фирмы и представителей других организационных структур в помещения фирмы, к конфиденциальным документам, делам, базам данных, компьютерам и средствам связи.

Контроль эффективности системы защиты информации – анализ степени *уязвимости конфиденциальной информации*.

Контроль доступа (Access auditing) – процесс защиты данных и программ от их использования объектами, не имеющими на это права.

Конфиденциальность (лат. *confidentia* – доверие) – доверительность, секретность. Не оглашаемая, доверительная, задушевная беседа, письмо, сообщение, полученное по доверенности, тайное общение, тайные переговоры, беседы, документирование с использованием *тайнописи*.

Конфиденциальная информация (Confidential information) – информация, доступ к которой ограничивается в соответствии с законодательством страны и уровнем доступа к информационному ресурсу. Конфиденциальная информация становится доступной или раскрытой только санкционированным лицам, объектам или процессам.

Криптография – тайнопись, система разнообразных способов изменения формы отображения информации (текста, речи),

позволяющих сделать содержание информации непонятным для лиц, не владеющих знанием использованного шифра.

Криптографический элемент системы защиты информации –комплекс способов и средств защиты *конфиденциальной информации* методами *криптографии*.

Лицензирование в области защиты информации – установленное законодательством право заниматься работами *по защите информации* для стороннего заказчика.

Машинограмма – документ, изготовленный автоматически средствами вычислительной техники (например, с помощью принтера) на бумажном *носителе* в человеко-читаемой форме и предназначенный для оформления в установленном порядке.

Метаданные (Metadata) – данные о данных: каталоги, справочники, реестры, базы метаданных, содержащие сведения о составе данных, содержании, статусе, происхождении, местонахождении, качестве, форматах и формах представления, условиях доступа, приобретения и использования, авторских, имущественных и смежных с ними правах на данные и др.

Методы защиты информации – выборочно применяемые универсальные и специфические способы (приемы, меры, мероприятия) реализации элементов *системы защиты информации* и входящих в них содержательных частей для формирования комплексной и индивидуальной структуры данной системы.

Методы легального получения информации – вид «невинного шпионажа», отличающийся правовой безопасностью, но предопределяющий возникновение интереса к конкурирующей фирме, необходимости обнаружения или формирования и использования *каналов несанкционированного доступа* к ее *ценной, конфиденциальной информации.*

Методы нелегального получения информации – всегда носят незаконный характер и используются в целях *несанкционированного доступа.*

Нарушение безопасности информации – событие, при котором компрометируется один или несколько аспектов безопасности информации (доступность, конфиденциальность, целостность и достоверность).

Нормативно-методическое обеспечение системы защиты информации – комплекс документов, регламентирующих процесс функционирования системы *защиты информации*, сформированной в целях *безопасности информации* конкретной фирмы, а также регламентирующих функционирование *службы безопасности* этой фирмы.

Обработка данных (Data processing; Performing data) – процесс выполнения последовательности операций над данными. Обработка данных может осуществляться в интерактивном и фоновом режимах.

Обработка изданных документов – технологическая стадия, в процессе которой выполняются технологические этапы процедуры и операции по отправке документов адресатам или передаче внутренних документов для использования в управлении основной деятельностью фирмы.

Обязательство о неразглашении конфиденциальных сведений – правовой документ, добровольное письменное согласие претендента на должность, сотрудника фирмы или иного лица на ограничение его права в отношении использования *конфиденциальной информации* фирмы.

Организационный элемент системы защиты информации – комплекс направлений и методов управленческого, ограничительного и технологического характера, определяющих основы и содержание *системы защиты*, побуждающих персонал соблюдать правила защиты конфиденциальной информации фирмы. Организационные меры связаны с установлением *режима конфиденциальности* в фирме.

Оформление и учет носителей конфиденциальной, информации –этап *стадии исполнения конфиденциального документа*. Осуществляется заблаговременно, т. е. до начала составления документа.

Персональные данные – информация о гражданах, лицах, особах, персонах, личностях, персоналиях, т. е. любая, в том числе недокументированная, информация, относящаяся к конкретному человеку.

Политика информационной безопасности (Security policy) – совокупность правил, определяющих и ограничивающих виды деятельности объектов и участников, системы информационной безопасности.

Пользователь (потребитель) информационных ресурсов – лицо (субъект), обращающееся к информационной системе или посреднику за получением необходимой ему информации и пользующееся ею. Пользователь не может участвовать в проектировании, модернизация или эксплуатации, *контроле эффективности системы защиты информации.*

Право информационное – совокупность законодательных информационно-правовых норм, регулирующих общественные отношения в информационной сфере и являющихся гарантированным инструментом охраны интеллектуальной информационной собственности *(информационного продукта)* юридических и физических лиц.

Правовой элемент системы защиты информации – юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования *системы защиты информации*, фирмы и персонала по поводу обязанности персонала соблюдать установленные *собственником* информации ограничительные и технологические меры защитного характера, а также ответственности персонала за нарушение порядка защиты информации.

Программно-аппаратный элемент системы защиты информации – комплекс специальных методов и средств *защиты информации* в автоматизированных системах и сетях.

Программный сервер, серверное программное обеспечение (server) – (англ. *server* от англ. *to serve* – служить) – в информационных технологиях – программный компонент вычислительной системы, выполняющий сервисные (обслуживающие) функции по запросу клиента, предоставляя ему доступ к определённым ресурсам или услугам. Пассивная сторона системы клиент-сервер.

Программное обеспечение (ПО) (Software) – комплекс программ, обеспечивающих обработку или передачу данных, предназначенных для многократного использования и применения разными пользователями.

Противодействие злоумышленнику – целенаправленное создание неблагоприятных условий и трудно преодолимых препятствий (рубежей) для лица, пытающегося совершить несанкционированный доступ и овладение конфиденциальной информацией фирмы. Может быть пассивным и активным. При пассивном противодействии *система защиты информации* функционирует в обычном режиме, ведется плановая аналитическая и контрольная работа с *источниками и каналами распространения информации, организационными и техническими каналами возможного несанкционированного доступа* к конфиденциальной информации. Активное противодействие предполагает подключение дополнительных организационных и *технических методов* защиты информации (например, закрытие доступа к определенным категориям информации, организацию усиленной охраны здания и помещений, ограничение деловых связей фирмы и др.).

Рабочая станция – периферийный компьютер в составе локальной вычислительной сети (ЛВС), играющий роль интерфейса по отношению к серверу.

Разглашение конфиденциальной информации – несанкционированный выход конфиденциальных сведений и документов за пределы круга лиц, которым они были доверены или стали известны по службе. Разглашение (огласка, оглашение) информации происходит по вине персонала – случайно, ошибочно или умышленно, добровольно (инициативно) или под воздействием угроз, шантажа, применения наркотических средств, психотропных препаратов.

Раздробление тайны – классифицированное (иерархическое) дробление предметной совокупности *конфиденциальной информации* на тематические группы, отдельные элементы, части, известные разным сотрудникам фирмы.

Разрешительная (разграничительная) система доступа к информации – совокупность обязательных норм, устанав-

ливаемых первым руководителем или коллективным органом руководства фирмой с целью закрепления за руководителями и сотрудниками права использования для выполнения служебных обязанностей *выделенных помещений*, рабочих мест, определенного состава документов и конфиденциальных сведений.

Режим конфиденциальности – комплекс мер, входящих в состав действующей в фирме *системы защиты информации* и обеспечивающих особый правовой статус организации работы сотрудников фирмы.

Секрет – см. *Тайна*.

Секретность данных (Secrecy) – свойство данных быть известными и доступными только тому кругу субъектов, для которого они предназначены.

Сервер баз данных, сервер БД – программное обеспечение, обслуживающее базу данных и отвечающее за целостность и сохранность данных, а также обеспечивающее операции ввода-вывода при доступе клиента к информации, то есть то же самое, что корпоративная СУБД.

Сервер доступа к данным – программный компонент СУБД, обслуживающий базу данных и отдающий данные по запросам.

Сервер-компьютер – компьютер, выполняющий только серверные задачи, или компьютер (или иное аппаратное обеспечение), специализированный (по форм-фактору и/или ресурсам) для использования в качестве аппаратной базы для программных серверов.

Сертификация систем и средств защиты информации – аналитические действия по определению эффективности *систем защиты информационных ресурсов*, качества программных, аппаратных и иных *средств защиты*. Выполняется специализированной организацией, имеющей соответствующую *лицензию*. В соответствии с положительными результатами анализа выдается сертификат, удостоверяющий возможность использования указанных систем и средств защиты для обеспечения *информационной безопасности* фирмы.

Система зашиты информации – совокупность направлений, методов, средств и мероприятий, снижающих *уязвимость информации* и препятствующих *несанкционированному доступу* к информации, *ее разглашению или утечке*.

Система обеспечения безопасности (Security system) – совокупность стандартных защитных мер: криптографическое кодирование, паролирование, присваивание идентификатора, электронная цифровая подпись и т.д.

Система охраны здания, помещений, транспорта и персонала – комплекс организационных и технических мероприятий, реализующих одну из основных функций *службы безопасности фирмы.*

Служба безопасности – самостоятельное структурное подразделение фирмы, обеспечивающее *экономическую безопасностью* функционирования. В негосударственных структурах подобная служба создается по усмотрению руководящего органа фирмы.

Справочно-информационный банк данных автоматизированный – структурированная совокупность сведений о документах, хранящихся в памяти ЭВМ.

Справочно-информационный банк данных по конфиденциальным документам – структурированная совокупность применяемых *учетных форм*.

Средства защиты информации – технические, криптографические, программные и другие средства, входящие в структуру отдельных элементов системы защиты информации и предназначенные для обеспечения защиты сведений, составляющих *тайну фирмы*, а также средства, в которых они реализованы, или предназначены для *контроля эффективности системы защиты информации.*

Сроки конфиденциальности информации – временной период ограничения доступа персонала и иных лиц *к конфиденциальной информации*. Характеризуется большим разбросом во времени – от нескольких часов до нескольких лет.

Структура данных (Data structure) – организационная схема записи или массива, в соответствии с которой упорядочены

данные, с тем чтобы их можно было интерпретировать и выполнять над ними определенные операции.

Тайнопись – см. *Криптография.*

Технические средства охраны, сигнализации и идентификации – специальные сооружения, оборудование и приборы, создающие препятствия на пути злоумышленника и оповещающие персонал охраны о попытке несанкционированного проникновения в здание фирмы, хранилища, другие охраняемые, *выделенные помещения*, к компьютерам, средствам связи.

Технологическая система обработки и хранения конфиденциальных документов – упорядоченный комплекс организационных и технологических процедур и операций, обеспечивающих служб и технических средств, предназначенных для практической реализации задач, стоящих пред функциональными элементами (стадиями) документопотока.

Технологическая система обработки и хранения конфиденциальных документов автоматизированная – комплекс организационных и технологических процедур и операций с документами, выполняемый на базе вычислительной техники и средств связи. Система, как и традиционная, делопроизводственная, обеспечивает конкретные потребности персонала *в конфиденциальной информации.*

Технология информационная защищенная – совокупность комплексных технологических систем, организационных структур, ограничительных методов и технических средств, предназначенных для традиционной и (или) автоматизированной обработки **конфиденциальной информации и документов**, решающих задачи информационного обеспечения управленческой и производственной деятельности в жестких условиях *информационной безопасности* обрабатываемых информационных ресурсов.

Угроза безопасности (Threat) – в широком смысле – потенциальное нарушение безопасности. Угроза безопасности – в системах обработки данных – потенциальное действие или событие, которое может привести к нарушению одного или более аспектов безопасности информационной системы.

Угроза безопасности конфиденциальной информации – единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или в*нутренних источников угрозы конфиденциальной информации* создавать неблагоприятные события, оказывать дестабилизирующее воздействие на *защищаемую информацию*.

Универсальный (сетевой) сервер – особый вид серверной программы, не предоставляющий никаких услуг самостоятельно. Вместо этого универсальные серверы предоставляют серверам услуг упрощенный интерфейс к ресурсам меж процессного взаимодействия и/или унифицированный доступ клиентов к различным услугам.

Уничтожение документов, дел и носителей информации – комплекс технологических приемов и правил, исключающих возможность *ознакомления посторонних лиц* с уничтожаемыми конфиденциальными материалами *или подмены* материалов.

Управление данными (Data management) – процесс, связанный с накоплением, организацией, запоминанием, обновлением, хранением данных и поиском информации.

Установление грифа конфиденциальности – этап *стадии исполнения конфиденциального документа* на любом *носителе*.

Утечка конфиденциальной информации – неконтролируемый выход *конфиденциальной информации за* пределы фирмы или охраняемой зоны. Связана с возможным перехватом информации злоумышленником с помощью технических средств разведки.

Утрата информацией конфиденциальности – переход информации в категорию общедоступной, известной конкуренту, информации открытого доступа. Санкционированной может быть только одна причина – снятие с традиционного или электронного документа *грифа конфиденциальности* в соответствии с установленными в фирме правилами. Несанкционированных причин может быть несколько, но все они являются следствием *утраты конфиденциальности информации*.

Уязвимость информации – объективное свойство информации подвергаться различного рода воздействиям (опасностям,

угрозам), нарушающим ее целостность, достоверность и *конфиденциальность.*

Файл-сервер – программный сервер для обеспечения доступа к файлам на диске сервера. Прежде всего это серверы передачи файлов по заказу, по протоколам FTP, TFTP, SFTP и HTTP. Протокол HTTP ориентирован на передачу текстовых файлов, но серверы могут отдавать в качестве запрошенных файлов и произвольные данные, например, динамически созданные веб-страницы, картинки, музыку и т.п.

Фальсификация документов – изготовление и использование в каких-либо целях ложного документа, в том числе злоумышленной *подмены* подлинного документа в целом или его отдельных частей поддельными, изготовленными для приобретения незаконных прав, выполнения противоправных действий в отношении фирмы или ее персонала.

Хакер (Hacker) (от англ. *Hack* – кромсать) – лицо, совершающее различного рода незаконные действия в сфере информатики, несанкционированное проникновение в чужие компьютерные сети и получение из них информации, незаконные снятие защиты с программных продуктов и их копирование, создание и распространения компьютерных вирусов и т.п. Действия хакера образуют различные составы уголовных преступлений и гражданских правонарушений.

Хранение конфиденциальных документов и дел – нахождение документов и дел в специальном хранилище, обеспечивающем их сохранность. Осуществляется *службой конфиденциальной документации* в отношении неисполненных и исполненных документов.

Целостность данных (Data integrity) – свойство, при выполнении которого данные сохраняют заранее определенный вид и качество.

Чувствительная информация (критическая информация) (Sensitive information) – информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к ощутимому убытку или (денежному) ущербу.

Шифр – совокупность условных знаков для преобразования информации в вид, исключающий ее восстановление (дешифрование и прочтение) в условиях отсутствия *у злоумышленника* ключа для раскрытия шифра.

Шифрование – криптографическое (математическое, алгоритмическое) преобразование информации с целью получения шифрованного текста или устной речи (см. также *Криптография*).

Шпионаж – похищение, добывание, собирание и передача с целью корыстного использования или выдачи конкуренту (противнику) сведений, составляющих *тайну*.

Шпионаж промышленный – получение предпринимателем самостоятельно или с помощью соответствующих специалистов (злоумышленников), обманным или иным незаконным *путем конфиденциальной информации* с целью овладения ею для достижения технического, технологического или коммерческого преимущества, банкротства конкурента.

Шпионаж экономический – широкое понятие, которое охватывает такие виды шпионажа, как промышленный, коммерческий, научно-технический, производственный и др.

Экстремальная (чрезвычайная) ситуация – явление, событие, нарушающее нормальное функционирование фирмы, работу персонала, создающее опасность для целостности и сохранности здания, помещений, оборудования и документации фирмы, угрожающее жизни и здоровью сотрудников. Экстремальные ситуации объективного характера связаны со стихийными бедствиями (ураганами, наводнениями и др.), неуправляемыми процессами, военными действиями, кризисами, авариями энергоснабжения и водоснабжения и другими подобными событиями. Экстремальные ситуации могут быть случайного (фатального) характера – возгорание оборудования и коммуникаций, разрушение конструкций, а также связаны с неосторожностью и безответственностью персонала (возгорания от неосторожного обращения с огнем, курения на рабочих местах, неумелой эксплуатации оборудования и др.).

ЛИТЕРАТУРА

1. *Акбай кызы А., Ордобаев Б.С.* Некоторые вопросы информационной безопасности и программного обеспечения. Ч. I. Общие понятия об информации: учебное методическое пособие. Бишкек: Изд-во КРСУ, 2018. 195.
2. *Дорофеев А.В.* Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С. 65–68.
3. https://ru.wikipedia.org/wiki.
4. CIS Security Benchmarks. Center for Internet Security, 2014. URL: https://benchmarks.cisecurity.org/downloads.
5. *Steven Hernandez.* Offi cial (ISC) 2 Guide to the CISSP CBK, Third Edition. ISC2 Press, 2012.
6. *James M. Stewart, Mike Chapple, Darril Gibson.* CISSP: Certifi ed Information Systems Security Professional Study Guide, 6th Edition. Sybex, 2012.
7. *Миронов В.* Древние цивилизации. М., 2006.
8. *Дандамаев М.А.* Нововавилонские документы об усыновлении // Scripta Gregoriana. М.: Вост. лит. РАН, 2003. С. 60–73.
9. *Shon Harris.* CISSP All-in-One Exam Guide, 6th Edition. McGrawHill, 2012.
10. *Сингх С.* Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006. 447 с.
11. *Бауэр Ф.* Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.
12. *Eric Conrad, Seth Misenar, Joshua Feldman.* CISSP Study Guide, Second Edition. Syngress, 2012.
13. *Акбай к. А., Ордобаев Б.С.* Некоторые вопросы информационной безопасности и программного обеспечения. Ч. II. Информационные технологии и офисные программы Windows: учебно-метод. пособие: Бишкек: Изд-во КРСУ, 2019.

Составители:
Акбай кызы Аида,
Ордобаев Бейшенбек Сыдыкбекович
Эргешов Эмиль

НЕКОТОРЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ЧАСТЬ III
ПРОГРАММНО-ТЕХНИЧЕСКИЕ СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. СУБД.

Учебно-методическое пособие

Редактор *К.В. Тимофеева*
Компьютерная верстка *А. Рахмановой*

Подписано в печать 25.07.2019
Печать офсетная. Формат 60 × 84 $^{1}/_{16}$.
Объем 6,75 п. л. Тираж 100 экз. Заказ 62

Издательство КРСУ
720000, г. Бишкек, ул. Киевская, 44

Отпечатано в типографии
720048, г. Бишкек, ул. Анкара, 2а