1. Структура информационного процесса.

1. Понятие информации, ее виды и свойства.
2. Структура информационного процесса.
3. Принципы обеспечения информационной безопасности.

1. Понятие информации, ее виды и свойства.

Информация является одним из фундаментальных понятий современности и относится к разряду тех, которые имеют очень широкое употребление. Информационные взаимодействия - это основа существования как живой, так и неживой природы. Без информационных процессов немыслима и социальная жизнь. Информационные технологии представляют собой основу информационного общества.

Термин «информация» *означает сведения, разъяснения, изложение.*

Обычно под информацией понимаются знания, сведения, сообщения и сигналы, с которыми мы имеем дело в повседневной жизни и проявление которых мы наблюдаем в природе и обществе.

Определение информации в энциклопедическом словаре – это общенаучное понятие, включающее обмен сведениями между людьми, обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму.

В Федеральном законе *«Об информации, информационных технологиях и о защите информации» информация - это сведения о лицах, предметах, фактах, событиях, процессах независимо от формы их представления».*

В научной литературе можно встретить десятки попыток дать определение «информации». Многие специалисты признают, что достаточно полного определения информации дать невозможно, что в каждой ситуации её определение имеет «своё лицо» и выполняет свои функции.

В философских работах информация *- это фундаментальная субстанция, стоящая в одном ряду с материей и энергией, а информационные взаимодействия –*

это формы процессов «отражения», присущих как материальному, так и духовному миру.

В естественных науках *информация - это ранее неизвестные знания об объектах и процессах окружающего нас мира.*

В процессе познания именно информация заставляет умножать наши знания. Естественно, что **ценность её всегда субъективна** и определяется возможностями потребителя, его целями, степенью его восприимчивости и уровнем его познаний.

В наше время **существует несколько подходов** к определению понятия «информация».

В связи с развитием средств связи, телекоммуникаций, вычислительной техники, их использованием для обработки и передачи информации, возникла необходимость измерять её **количественные характеристики.**

Так, ***в первом подходе различают разные меры информации:***

- *техническая мера - информация, которая передается по телеграфным линиям и отображается на экранах радиолокаторов. Количество информации может быть точно вычислено, и ее процессы подчиняются физическим законам.* По сути, при таком измерении информация отождествляется с данными;

- *семантическая мера* т.е. смысловая - *информация, которая содержится в литературном произведении.* Информация отождествляется со сведениями и фактами.

Второй подход состоит в том*, что информация - это характеристика, такая же, как энергия или масса в физике. Определенным образом и в определенных условиях информация равным образом описывает как процессы, происходящие в естественных физических системах, так и процессы, происходящие в искусственно созданных системах.*

Третий подход состоит в том*, что информация как объект едина, но следует оценивать качественные показатели, которые определяют ее ценность: достоверность, актуальность, надёжность.*

Учитывая сказанное выше, следует:

Информация - *сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы (живые организмы, управляющие машины) в процессе жизнедеятельности и работы.*

Информация может существовать в виде текстов, рисунков, чертежей, фотографий, световых или звуковых сигналов, электрических импульсов, магнитных записей, жестов и мимики, запахов и вкусовых ощущений и т.д.

На практике часто отождествляются определения таких понятий, как «информация», «данные», «знания». Однако эти понятия необходимо различать.

Данные - *фиксируемые в виде определенных сигналов воспринимаемые факты окружающего мира.*

Данные несут в себе сведения о событиях, произошедших в материальном мире, и являются регистрацией сигналов, возникших в результате этих событий.

Однако станут ли данные информацией – зависит от того, известен ли метод преобразования данных в известные понятия.

Например, мы можем услышать речь обращающегося к нам человека на иностранном языке. С одной стороны, мы получили от него данные в виде звуков, но с другой - никакой информации от него мы получить не смогли, т.к. не сумели понять передаваемые нам данные. Они для нас были закодированы.

Знание - *это осознание, понимание и толкование определенной информации с учетом путей наилучшего ее использования для достижения конкретных целей.*

Информацию человек может получать откуда угодно, а знания приходят, когда человек использует эту информацию и сочетает ее со своим собственным опытом. Информация становится знанием, когда она переработана и проанализирована человеческим мозгом.

Знания должны иметь структуру и связь между собой, а не быть хаотичными.

Виды знания: *научное, обыденное (здравый смысл), интуитивное, религиозное и др.*

Обыденное знание *служит основой ориентации человека в окружающем мире, основой повседневного поведения, но содержит ошибки и противоречия.*

Научному знанию *присущи логическая обоснованность, доказательность, воспроизводимость результатов, проверяемость, стремление к устранению ошибок и преодолению противоречий.*

Можно сделать вывод, что *фиксируемые воспринимаемые факты окружающего мира представляют собой данные. При использовании данных в процессе решения конкретных задач - появляется информация. Истинная, проверенная информация, обобщенная в виде законов, совокупностей взглядов и понятий представляет собой знания.*

Информацию можно упорядочить по ряду признаков, т.е. провести ее классификацию.

Классификация информации:

1. По способам восприятия:

Визуальная, Аудиальная, Тактильная, Обонятельная, Вкусовая

2. По форме представления:

Буквенная, Цифровая, Графическая, Кодированная, Комбинированная

3. По форме передачи:

Вербальная (словесная, звуковая), *Невербальная* (представленная на определенном носителе: бумаге, дискете и т.д.)*, Письменная, Печатная, Телефонная, Электронная, Спутниковая и т.д.*

4. По назначению: *Экономическая**,** Техническая**,** Социальная**,** Организационная.*

5. По общественному значению:

- *Массовая: Обыденная, Общественно-политическая, Эстетическая*
- *Личная: Знания, Интуиция*
- *Специальная: Научная, Производственная, Техническая, Управленческая*

6. По изменчивости во времени:

Условно-постоянная (например, место жительства человека)

Условно-переменная (например, последовательность календарных месяцев)

Постоянная (например, дата рождения человека)

Переменная

7. По режиму передачи от одного потребителя информации другому:

В произвольные сроки, По запросу, Принудительно в определенные сроки.

Как и всякий объект, информация обладает **свойствами**. На свойства информации влияют **свойства исходных данных**, составляющих ее содержательную часть и **свойства методов**, фиксирующих эту информацию.

Группы свойств информации:

***1. Атрибутивные свойства* - без которых информация не существует:**

- Дискретность - отдельные данные, которые распространяются в виде сообщений из линий, цвета, букв, цифр, символов, знаков.

- Непрерывность. Информация имеет свойство сливаться с уже зафиксированной и накопленной ранее, способствуя развитию и накоплению.

- Передаваемостъ с помощью каналов связи: способность информации к копированию, т.е. к тому, что она может быть «запомнена» другой системой и при этом останется тождественной самой себе.

- Преобразуемость - информация может менять способ и форму своего существования.

***2. Прагматические свойства* - характеризуют степень полезности информации для пользователя:**

- Адекватность - степень соответствия реальному объективному состоянию дела Неадекватная информация может образовываться на основе недостоверных данных. Однако и достоверные данные могут приводить к созданию неадекватной информации в случае применения к ним неадекватных методов.

- Актуальность (важность для настоящего времени) - *степень соответствия информации текущему моменту времени.* Только вовремя полученная информация может быть полезна.

- Доступность - возможность получения информации потребителем.

- Защищенность - невозможность несанкционированного использования или изменения информации.

- Достоверность - истинное положение дел. Но достоверная информация может быть как объективной, так и субъективной. Достоверная информация помогает принять нам правильное решение.

Причины недостоверной информации:

-преднамеренное искажение (дезинформация);

- искажение в результате воздействия помех («испорченный телефон»).

- *Объективность и субъективность. Информация объективна, если она не зависит от методов ее фиксации, чьего-либо мнения, суждения.*

Объективную информацию можно получить с помощью датчиков, измерительных приборов. *В сознании человека информация преобразовывается в зависимости от мнения, суждения, опыта, знаний конкретного субъекта.* В ходе информационного процесса степень объективности информации всегда понижается.

- *Полезность. Уменьшение неопределенности сведений об объекте.* Полезность оценивается по тем задачам, которые можно решить с ее помощью.

- *Полнота - определяет достаточность данных для принятия решений.* Неполная информация может привести к ошибочному выводу или решению.

- *Релевантность - способность информации соответствовать запросам потребителя.*

- *Ценность. Самая ценная информация - объективная, достоверная, полная и актуальная.* Ценность информации различна для различных потребителей и пользователей. При этом следует учитывать, что и необъективная информация (например, художественная литература), имеет большую значимость для человека.

- *Эргономичность - удобство формы информации с точки зрения данного потребителя.*

***3. Динамические свойства* - которые характеризуют изменение информации во времени:**

- *Кумулятивность* (увеличение, скопление) - *характеризует накопление и хранение информации.*

- *Рост информации. С течением времени количество информации накапливается, происходит ее систематизация, оценка и обобщение.*

- *Старение – уменьшение ценности информации с течением времени.* Информация подвержена влиянию времени. Старит информацию не само время, а появление новой информации, которая **уточняет, дополняет или отвергает** более раннюю.

Научнотехническая информация стареет быстрее, эстетическая (произведения искусства) - медленнее.

- *Стираемостъ - преобразование информации* (передача), *при котором ее количество уменьшается и становится равным нулю.*

- Запоминаемость. С запоминаемой информацией мы имеем дело только в реальной практике.

2. Структура информационного процесса.

Те предметы или устройства, от которых человек может получить информацию, называют ***источниками информации.***

Те предметы или устройства, которые могут получать информацию, называют ***приёмниками информации.***

Сообщение, отображающее информацию, всегда представляется в виде сигнала.

Сигнал - *изменение состояния некоторого объекта.*

При переносе информации *в виде сигнала от источника к приёмнику* (потребителю) *она последовательно проходит фазы обращения, составляющие* ***информационный процесс:***

1. ***Получение информации*** *– сбор сведений, из доступных восприятию источников – химический состав среды, электромагнитный сигнал, зрение, слух, флеш-карта и т.п.* Как видно, в первую очередь тут важен именно физический способ восприятия информации и ее передачи. Человек никак не воспринимает окружающие его радиоволны, а радиоприемник не способен воспринимать звук, хотя и может его генерировать.

Но для конкретного человека неотъемлемой частью получения информации является ***актуальность,*** *выраженная в цели и источнике.* Археолог не сделает никаких открытий, копаясь в социальных сетях. Однако рекламщику социальные сети будут полезны. Несмотря на то, что в обоих случаях оба получают одинаковую информацию, для одного этот процесс совершенно бессмысленный.

2. ***Обработка информации*** *– алгоритм преобразования информации в данные.* Информационный процесс совершенно точно изменит исходную информацию. Фактически анализ информации один из самых сложных и малопонятных механизмов на планете — человеческий мозг — предназначен именно для этого.

В радиоприемнике радиоволны превращаются в звуковые, свет через глаза попав в мозг становится визуальными образами, набор электрических сигналов в мозгу преобразуется в мысль, а затем в звуковые сигналы речи.

В анализе информации состоит основная разница информационного процесса в биологии и информатике. **Биологические объекты** (человек) интерпретируют полученную информацию, дают оценку и реакцию.

А **магнитофон** только запишет звук, ничего не интерпретируя.

3. ***Сохранение информации*** *– любые действия для того, чтобы полученные после обработки данные могли быть использованы в дальнейшем, начиная от памяти живых организмов и заканчивая электронными носителями.*

Сюда же могут входить любые действия, препятствующие нежелательному использованию сохраненных сведений, начиная от закапывания тайных книг и заканчивая современными криптографическими методами.

Эффективность этого шага напрямую зависит от используемых методов и технологий – чем лучше технология, тем надежнее сохранена информация.

4. ***Коммуникации*** *– процесс передачи информации другим субъектам.* Каждый информационный процесс подразумевает под собой передачу полученной информации кому-либо другому, будь то человек или машина для ее дальнейшего использования.

Что характерно, ***информация не имеет значения****, если она не была как-то кем-то использована.*

Очевидно, что установка счетчика на водяную трубу бессмысленна, если счетчик не оборудован табло с цифрами. Написание автором романа и сокрытие его бессмысленно.

Фактически, *коммуникация является логическим завершением информационного процесса, действием придающим смысл всему*.

По сути, коммуникация - то, что отличает информационный процесс от похожих процессов в неживой природе — вещества в химической реакции меняют цвет не «для чего-то», а «потому-то». А любой информационный процесс происходит исключительно с какой-то конечной целью.

3. Принципы обеспечения информационной безопасности

Организация информационной безопасности предполагает разработку определённых принципов её обеспечения.

Принцип баланса интересов личности, общества и государства.

Личность заинтересована в конфиденциальности информации об интимной жизни, доходах и т.д., а общество заинтересовано в получении сведений об антисоциальных проявлениях, коррупции, преступных доходах и т.д.

Принцип законности и правой обеспеченности. Рост значимости ИБ опережает развитие соответствующей сферы права, чем умело пользуются и политики, и преступники. СМИ не несут никакой ответственности за ложную информацию, направленную на массового потребителя этой информации (читателя, телезрителя).

Принцип интеграции с международными системами безопасности информации. *Глобализация - процесс всемирной экономической, политической и культурной интеграции.* Глобализация требует развития международных коммуникаций и их согласованности в обеспечении безопасности передачи информации.

Принцип экономической эффективности - *результаты от мер ИБ должны превышать затраты на них.* Если этот принцип не соблюдается, то меры по обеспечению секретности информации не окупаются и вредят прогрессу.

Принцип мобильности системы ИБ. *Система ИБ не должна допускать неоправданных режимных ограничений, т.к. государство утрачивает возможность защищать, создавать и генерировать новые знания.*

Принцип презумпции несекретности информации *означает, что строгому нормированию подлежит конфиденциальность, а не гласность.*

Принцип невозможности миновать защитные средства говорит сам за себя и не требует дополнительных пояснений.

Принцип усиления самого слабого звена. Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения ИБ приобретает нетехнический характер.

Принцип невозможности перехода в небезопасное состояние *означает, что при любых нештатных обстоятельствах защитное средство либо полностью выполняет свои функции, либо блокирует доступ.*

Принцип минимизации привилегий - *выделение администраторам и пользователям только те права доступа, которые необходимы для выполнения служебных обязанностей.* Назначение этого принципа - уменьшить ущерб от случайных или умышленных некорректных действий.

Принцип разделения обязанностей - *распределение ответственности, чтобы один человек не мог нарушить важный для организации процесс или создать брешь в защите по заказу злоумышленников.*

Принцип эшелонированности обороны *– наличие нескольких защитных рубежей. За средствами физической защиты должны следовать программно-технические средства, за идентификацией - управление доступом, протоколирование и аудит.* Эшелонированная оборона способна задержать злоумышленника, а наличие протоколирования и аудита существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств - *организация различных по характеру оборонительных рубежей.* Чтобы от потенциального злоумышленника требовалось овладение разнообразными и несовместимыми между собой навыками.

Принцип простоты и управляемости информационной системы. *Залогом ИБ являются не сложность и скрытность, а простота и апробированность.* Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществить централизованное администрирование.

Принцип обеспечения всеобщей поддержки мер безопасности носит нетехнический характер. Если системные администраторы считают ИБ чем-то излишним, режим безопасности сформировать не удастся.

Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное теоретическое и практическое обучение.

2. Информационная безопасность: понятие, значение

1. Понятие информационной безопасности
2. Информационные опасности и угрозы
3. Восприятие информации человеком

1. Понятие информационной безопасности

В повседневной жизни часто ИБ понимается лишь как необходимость борьбы с утечкой секретной и распространением ложной информации. Однако это понимание очень узкое. Существует много разных определений ИБ, в которых высвечиваются отдельные её свойства. Достаточно полным определением является:

Информационная безопасность *- защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.*

Следует отличать информационную безопасность от защиты информации.

Защита информации *- деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.*

Иногда под защитой информации понимается создание в ЭВМ организованной совокупности средств, методов и мероприятий, предназначенных для предупреждения, уничтожения или несанкционированного использования защищаемой информации.

Международный день защиты информации - 30 ноября. Отмечается с 1988 года, когда произошла первая массовая компьютерная эпидемия червя Морриса. Америка была в шоке, когда практически все компьютеры, имевшие доступ к интернету, «зависли» на несколько дней. Сначала это отнесли к сбоям в энергосистеме. Но потом стало ясно, что терминалы были атакованы неизвестной на тот момент программой, содержавшей код, не поддающийся имеющимися средствами расшифровке. Сам вирус этого типа явился первым в своем роде. Именно он стал родоначальником всех остальных программ такого типа. **«Червь Морриса» изначально был создан как средство тестирования уязвимостей систем** Робертом Моррисом (программистом).

Меры по обеспечению ИБ *должны осуществляться в разных сферах - политике, экономике, обороне, а также на различных уровнях - государственном, региональном, организационном и личностном.*

Поэтому задачи ИБ на уровне государства отличаются от задач, стоящих перед ИБ на уровне организации.

Субъект информационных отношений в организации *может пострадать от несанкционированного доступа к информации, от поломки системы, от поддерживающей инфраструктуры* (системы электро-, водо- и теплоснабжения, кондиционеры, обслуживающий персонал). Поддерживающая инфраструктура имеет

самостоятельную ценность, важность которой переоценить невозможно.

После событий 11 сентября 2001 года в законодательстве США было определено понятие «критическая инфраструктура», которая понимается как «совокупность систем и средств, важных в такой мере, что их выход из строя или уничтожение могут привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации».

В социальном плане ИБ *- это борьба с информационным «загрязнением» окружающей среды, использованием информации в противоправных и аморальных целях****. Объект ИБ*** *- информация, затрагивающая государственные, служебные, коммерческие, интеллектуальные и личностные интересы.*

Также объектами информационного воздействия могут быть общественное или индивидуальное сознание.

Общественное сознание *- совокупность идей, взглядов, представлений, существующих в обществе в данный период, в которых отражается социальная действительность.*

Субъекты ИБ *– органы исполнительной, законодательной и судебной власти; структуры, которые занимаются обеспечением ИБ; граждане и общественные объединения; СМИ; предприятия и организации.*

Интересы субъектов ИБ подразделяют на категории:

Доступность - *возможность за приемлемое время получить требуемую информационную услугу.*

Информационные системы создаются для получения определенных информационных услуг. Если получение услуг пользователями становится невозможным, это наносит ущерб всем субъектам информационных отношений. Поэтому доступность является важнейшим элементом ИБ.

Целостность - *актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.*

Целостность подразделяется:

- на статическую (понимаемую как неизменность информационных объектов)

- на динамическую (относящуюся к корректному выполнению сложных действий (транзакций)).

Практически все нормативные документы относятся к статической целостности. Пример динамической целостности - анализ потока финансовых сообщений с целью выявления кражи или переупорядочения.

Конфиденциальность *- защита от несанкционированного ознакомления.* На страже конфиденциальности стоят законы и нормативные акты. Также аппаратно-программные продукты позволяют закрыть практически все потенциальные каналы утечки информации.

Цель мероприятий в области информационной безопасности - защита интересов субъектов ИБ.

Задачи ИБ:

1. Обеспечение права личности и общества на получение информации.

2. Обеспечение объективной информацией.

3. Борьба с криминальными угрозами в сфере информационных систем, с телефонным терроризмом, отмыванием денег и т.д.

4. Защита личности, организации, общества и государства от информационно-психологических угроз.

5. Формирование имиджа, борьба с клеветой, слухами, дезинформацией.

Критерий ИБ *- гарантированная защищённость информации от утечки, искажения, утраты или иных форм обесценивания.* Безопасные информационные технологии должны обладать способностью к недопущению или нейтрализации внешних и внутренних угроз информации и содержать в себе адекватные методы и способы её защиты.

2. Информационные опасности и угрозы

Создание системы ИБ предполагает выявление источников информационных опасностей и угроз.

Информация подвергается угрозам во время сбора, модификации (искажение), утечки и уничтожения информации.

Внешние и внутренние источники информационных угроз:

Источниками внутренних угроз являются:

1. Сотрудники организации

2. Программное обеспечение

3. Аппаратные средства

Внутренние угрозы могут проявляться в следующих формах:

- ошибки пользователей и системных администраторов;

- нарушения сотрудниками установленных регламентов сбора, обработки, передачи и уничтожения информации;

- ошибки в работе программного обеспечения;

- сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

1. Компьютерные вирусы и вредоносные программы

2. Организации и отдельные лица

3. Стихийные бедствия

Формами проявления внешних угроз являются:

- заражение компьютеров вирусами;

- несанкционированный доступ к корпоративной информации;

- информационный мониторинг (со стороны конкурирующих структур, разведывательных и специальных служб);

- действия государственных служб, сопровождающиеся сбором, изъятием и уничтожением информации;

- аварии, пожары, техногенные катастрофы, стихийные бедствия.

Все виды угроз (формы проявления) *можно разделить на* ***умышленные и неумышленные.***

По стат. данным **свыше 50% вторжений** - дело рук собственных сотрудников компаний. Несанкционированное изменение данных наиболее часто применялось против **медицинских и финансовых** учреждений. Такими злоумышленниками наиболее часто являются **обиженные служащие и конкуренты**.

По способам воздействия на объекты ИБ угрозы классифицируются: *информационные, программные, физические, радиоэлектронные и организационно-правовые.*

К информационным угрозам относятся:

- несанкционированный доступ к информационным ресурсам;

- незаконное копирование данных;

- хищение информации;

- нарушение технологии обработки информации;

- противозаконный сбор и использование информации;

- использование информационного оружия.

К программным угрозам относятся:

- использование ошибок в программном обеспечении;

- компьютерные вирусы;

- установка «закладных» устройств (перехват информации).

К физическим угрозам относятся:

- разрушение средств обработки информации и связи;

- хищение носителей информации;

- хищение программных ключей и средств криптографической защиты данных;

- воздействие на персонал.

К радиоэлектронным угрозам относятся:

- внедрение электронных устройств в помещения;

- перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К организационно-правовым угрозам относятся:

- нарушение требований законодательства;

- задержка в принятии необходимых нормативно-правовых решений в информационной сфере;

- закупки устаревших информационных технологий и средств информатизации.

Информатизация *- организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, организаций, общественных объединений на основе формирования и использования информационных ресурсов.*

Защита интересов субъектов информационных отношений происходит на уровнях:

1) законодательный уровень: *регламентация законом и нормативными актами действий с информацией и оборудованием, и наступление ответственности нарушение правильности таких действий (законы, нормативные акты, стандарты и т.п.).* Законодательный уровень является важнейшим для обеспечения информационной безопасности.

2) административный уровень: *формирование программы работ в области информационной безопасности и обеспечение ее выполнения, выделяя необходимые ресурсы и контролируя состояние дел* (действия общего характера,

предпринимаемые руководством организации). Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

3) процедурный уровень (конкретные меры безопасности, ориентированные на людей).

Меры данного уровня включают в себя:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;

- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);

- мероприятия, осуществляемые при подборе и подготовке персонала, обслуживающего систему;

- организацию охраны и режима допуска к системе;

- организацию учета, хранения, использования и уничтожения документов и носителей информации;

- распределение реквизитов разграничения доступа;

- организацию явного и скрытого контроля за работой пользователей;

- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения.

4) программно-технический уровень (технические меры): *использование специальных программ и аппаратуры и выполняющих* (самостоятельно или в комплексе с другими средствами) *функции защиты*:

- идентификацию и аутентификацию пользователей;

- разграничение доступа к ресурсам;

- регистрацию событий;

- криптографические преобразования;

- проверку целостности системы;

- проверку отсутствия вредоносных программ;

- программную защиту передаваемой информации и каналов связи;

- защиту системы от наличия и появления нежелательной информации;

- создание физических препятствий на путях проникновения нарушителей;

- мониторинг и сигнализацию соблюдения правильности работы системы;

- создание резервных копий ценной информации.

3. Восприятие информации человеком

Анализаторы (система чувствительных нервных образований: зрительный, слуховой, вестибулярный, вкусовой, обонятельный, кожный, мышечный и другие) являются специальными структурами организма, служащими для ввода внешней информации в мозг для последующей ее переработки. Человек связан со средой с помощью анализаторов, которые состоят из рецепторов, проводящих нервных путей в коре головного мозга.

Например, когда человек ест, то он чувствует вкус, запах пищи и ощущает её температуру.

Основная характеристика анализаторов - **чувствительность.**

У человека рецепторы настроены на следующие раздражители:

- *фоторецепторы в сетчатке глаза* (электромагнитные колебания светового диапазона);

- *рецепторы вестибулярного аппарата* (изменение положения тела относительно вектора гравитации);

- *фонорецепторы уха* (механические колебания воздуха);

- *баро- и осморецепторы* (изменение гидростатического и осмотического давления крови);

- *хеморецепторы* (воздействие химических веществ);

- *терморецепторы* (температурные изменения как внутри организма, так и в окружающей среде);

- *тактильные и болевые рецепторы.*

В ответ на изменение условий окружающей среды, чтобы внешние раздражители не вызывали повреждений и гибели организма, в нём формируются ***компенсаторные реакции,*** *которые могут быть:*

- *поведенческими* (изменение места пребывания, отдёргивание руки от горячего или холодного)
- *внутренними* (изменение механизма терморегуляции в ответ на изменение параметров микроклимата).

Человек обладает органами чувств, обеспечивающими восприятие воздействующих на организм внешних раздражителей (органы зрения, слуха, обоняния, вкуса, осязания). **Нельзя путать понятия «органы чувств» и «рецептор».**

Например, **глаз - это орган зрения, а сетчатка - фоторецептор**, один из компонентов органа зрения.

Органы чувств сами по себе не могут обеспечить ощущение. Для возникновения ощущения необходимо, чтобы возбуждение в рецепторах, поступило в соответствующий отдел коры больших полушарий.

Зрение - *ведущий источник информации для человека (90% информации об окружающей среде).* Мы знаем, как трудно ориентироваться в условиях абсолютной темноты.

Визуальная среда, с которой человек соприкасается каждый день, влияет на зрение человека, оказывая воздействие и на его самочувствие.

Неблагоприятная визуальная среда может вызывать у человека раздражение, приводить к тяжелым психическим расстройствам.

Изучением окружающей видимой среды как экологического фактора занимается ***видеоэкология.***

Большое значение в восприятии человеком окружающей среды имеет осязание. ***Осязание*** *- сложное ощущение, возникающее при раздражении рецепторов кожи, наружных частей слизистых оболочек и мышечно-суставного аппарата. Кожный анализатор воспринимает внешние механические, температурные, химические и другие раздражители кожи.*

Осязание дополняет зрение в том смысле, что дает информацию об изменении осязательных аспектов окружающей среды.

Путем исследований доказано, что человек может жить, потеряв зрение, но без осязания, точки которого рассеяны по всей поверхности тела, он жить не может.

Мы постоянно соприкасаемся с чем-то: с одеждой, с предметами, с которыми работаем. Осязание позволяет чувствовать сопротивление и давление и не зависит от нашего воображения. Таким образом, осязание постоянно информирует нас об особенностях окружающей среды.

Слух - *пассивный орган в процессе восприятия, способность организма принимать и различать звуковые колебания слуховым анализатором.*

Слух дает нам информацию о среде, которая находится вне нашего зрительного поля, за горизонтом, охватываемым зрением. **Восприятие** пространства в значительной мере **зависит от функции слухового аппарата**, регистрирующего приятные и неприятные звуки, например шум, который относится к типу **невротического влияния окружающей среды**.

Шумовое загрязнение *- форма физического загрязнения, возникающего в результате увеличения интенсивности и повторяемости шума сверх природного уровня.*

Приводит к повышению утомляемости человека, снижению умственной активности и при достижении 100 дБ к постепенной потере слуха.

Обоняние *- способность воспринимать запахи.* Человек обладает разной степенью обоняния к различным пахучим веществам. Приятные запахи улучшают самочувствие человека, а неприятные действуют угнетающе, вызывают отрицательные реакции вплоть до тошноты, рвоты, обморока (сероводород, бензин), способны изменять температуру кожи, вызывать отвращение к пище, приводить к подавленности и раздражительности.

Грудной ребёнок, которому всего несколько дней, может четко различать одежду матери, при этом он руководствуется только обонянием.

В городской среде у человека подсознательно уменьшается чувствительность органа обоняния. Воздух здесь наполнен таким количеством отработанных газов, что людям ничего не остается, как только постепенно привыкать к ним.

Пригодность среды для выполнения определенной деятельности человек оценивает, как правило, носом, который по запахам получает информацию там, где глаз не видит, и откуда не доносятся акустические сигналы.

Например, легкое ощущение знакомого запаха может вызвать четкие воспоминания о чем-то давно минувшем, например в памяти всплывает живое представление определенной ситуации.

Вкус - *ощущение, возникающее при воздействии определённых химических веществ на вкусовые рецепторы, расположенные на различных участках языка.*

Вкус складывается из ***четырёх простых вкусовых ощущений****: кислое, солёное, сладкое и горькое.* Все остальные вариации вкуса – это комбинации из основных ощущений.

Восприятие окружающей среды происходит путем ***одновременного взаимодействия*** *всех органов чувств,* хотя человек все более становится рабом зрения. Это усиленно закрепляет сегодня аудиовизуальный характер культуры, где на первом месте стоит телевидение, современный человек в своей оценке окружающей среды все больше полагается на зрение.

Есть ли у человека наряду с классическими пятью органами чувств, другие органы, с помощью которых он может ориентироваться в жизненной среде и получать информацию?

В 1976 г. было проведено **исследование скрытых способностей человека** ориентироваться в незнакомой среде. В этом эксперименте приняли участие 64 студента. Им завязали глаза темной материей и посадили в автобус. Затем автобус отправился по сложному маршруту. Проехав 50 км, автобус остановился, и студенты вышли с завязанными глазами.

Их задачей было ответить на вопрос: **в каком направлении расположен университет?** Только после этого с них сняли повязку и попросили показать, на этот раз с открытыми глазами, где находится университет.

Согласно результатам исследования, определение направления, сторон света было более правильным, когда они отвечали с повязкой на глазах.

Когда у студентов сняли повязку, то точность ответа исчезла.

Таким образом, подтверждена гипотеза: ***человек также обладает органом****, воспринимающим действие магнитного поля, в ориентировании в незнакомой местности и в определении направления исходной точки.*

Конфиденциальная информация и её защита

Коммерческая тайна

Служебная тайна

Профессиональные тайны

Персональные данные

С развитием информационного общества проблемы, связанные с защитой конфиденциальной информации, приобретают

всё большее значение. В настоящее время в российском законодательстве данные вопросы полно и системно не решены. Развернутая классификация конфиденциальной информации, как

уже говорилось выше, приводится в перечне сведений конфиденциального характера, установленном Указом Президента РФ

от 6 марта 1997 г. № 188. Далее мы рассмотрим более подробно

некоторые виды конфиденциальной информации.

Коммерческая тайна

Коммерческая деятельность организации тесно связана с

получением, накоплением, хранением, обработкой и использованием разнообразной информации. Защите подлежит не вся

информация, а только та, которая представляет ценность для

организации. При определении ценности коммерческой информации необходимо руководствоваться такими её свойствами,

как полезность, своевременность и достоверность.

Полезность информации состоит в том, что она создает

субъекту выгодные условия для принятия оперативного решения и получения эффективного результата. В свою очередь полезность информации зависит от своевременного её получения и

доведения до исполнителя. Из-за несвоевременного поступления важных по своему содержанию сведений часто упускается

возможность заключить выгодную торговую или иную сделку.

Критерии полезности и своевременности тесно взаимосвязаны и взаимозависимы с критерием достоверности информации. Причины возникновения недостоверных сведений различны: неправильное восприятие (в силу заблуждения, недостаточного опыта или профессиональных знаний) фактов или умышленное, предпринятое с определенной целью, их искажение. Поэтому, как правило, сведения, представляющие коммерческий

интерес, а также источник их поступления должны подвергаться

перепроверке.

Коммерческая (служебная) тайна негосударственной

организации - сведения, не являющиеся государственными секретами, которые связаны с производственной, управленческой, финансовой или иной деятельностью организации и распространение которых может

нанести ущерб её интересам._____

Собственник коммерческой информации на основании совокупности перечисленных критериев определяет её ценность

для своей хозяйственной деятельности и принимает соответствующее оперативное решение.

В зарубежной экономической литературе коммерческая

информация рассматривается не в качестве средства извлечения

прибыли, а, прежде всего, как условие, способствующее или

препятствующее получению прибыли. Особо подчеркивается

наличие стоимостного фактора коммерческой информации, т.е.

возможность выступать в качестве предмета купли-продажи.

Поэтому важное значение в условиях развития многообразных

форм собственности имеет вопрос об определении принадлежности информации на правах интеллектуальной собственности

конкретному субъекту предпринимательства, а в итоге - о наличии у него прав на её защиту.

Определение и вопросы гражданско-правовой защиты

служебной и коммерческой тайны в российском законодательстве не различаются и рассмотрены в ст. 139 части первой ГК

РФ, называющейся «Служебная и коммерческая тайна»:

«Информация составляет служебную или коммерческую

тайну в случае, когда информация имеет действительную или

потенциальную коммерческую ценность в силу неизвестности

её третьим лицам, к ней нет свободного доступа на законном

основании и обладатель информации принимает меры к охране

её конфиденциальности. Сведения, которые не могут составлять

служебную или коммерческую тайну, определяются законом и

иными правовыми актами.

Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию,

которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданскоправовому договору».

Обеспечение защиты государственной тайны не имеет

прямого отношения к защите коммерческой тайны. Однако следует указать на некоторые возможные исключения. Под защиту

государства может быть взята коммерческая информация, оцененная как особо важная не только для её собственника, но и

для государства, когда не исключено, что к ней может проявить

интерес иностранная спецслужба. Вопрос о подобной защите

должен решаться на договорной основе между предпринимателем и органом федеральной безопасности с обозначением пределов и функций профессиональной деятельности последних.

Что касается собственно коммерческой тайны, то она специальной уголовно-правовой и режимной защитой не обладает.

Действительная или потенциальная коммерческая ценность информации во многом носит субъективный характер и

позволяет предпринимателю ограничивать доступ к практически любым сведениям, используемым в предпринимательской

деятельности, за исключением сведений, определяемых нормативно-правовым и актами.

Какие сведения не могут составлять коммерческую тайну?

В постановлении Правительства РСФСР от 5 декабря 1991 г. №

35 «О перечне сведений, которые не могут составлять коммерческую тайну» обозначены:

- учредительные документы (решение о создании предприятия или договор учредителей) и Устав;

- документы, дающие право заниматься предпринимательской (деятельностью (регистрационные удостоверения, лицензии, патенты);

- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов

и других обязательных платежей в государственную бюджетную систему РСФСР;

- документы о платежеспособности;

- сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных

рабочих мест;

- документы об уплате налогов и обязательных платежах;

- сведения о загрязнении окружающей среды, нарушении

антимонопольного законодательства, несоблюдении безопасных

условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства

РСФСР и размерах причиненного при этом ущерба;

- сведения об участии должностных лиц предприятия в

кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

Этим же нормативным актом запрещено государственным

и муниципальным предприятиям до и в процессе их приватизации относить к коммерческой тайне данные:

- о размерах имущества предприятия и его денежных

средствах;

- о вложении средств в доходные активы (ценные бумаги)

других предприятий, в процентные облигации и займы, в уставные фонды совместных предприятий;

- о кредитных, торговых и иных обязательствах предприятия, вытекающих из законодательства РСФСР и заключенных

им договоров;

- о договорах с кооперативами, иными негосударственными предприятиями, творческими и временными трудовыми коллективами, а также отдельными гражданами.

Следует отметить, что ограничения, вводимые на использование сведений, составляющих коммерческую тайну, направлены на защиту интеллектуальной, материальной, финансовой

собственности и других интересов, возникающих при формировании трудовой деятельности организации, персонала подразделений, а также при их сотрудничестве с работниками других

организаций.

Целью таких ограничений является предотвращение разглашения, утечки или несанкционированного доступа к конфиденциальной информации. Ограничения должны быть целесообразными и обоснованными с точки зрения необходимости

обеспечения информационной безопасности. Не допускается

использование ограничений для сокрытия ошибок и некомпетентности руководства организации, расточительства, недобросовестной конкуренции и других негативных явлений в деятельности организации, а также для уклонения от выполнения

договорных обязательств и уплаты налогов.

Служебная тайна

Если основной целью обеспечения конфиденциальности

информации, составляющей коммерческую тайну, является

обеспечение конкурентного превосходства, то защита конфиденциальности служебной тайны, хотя и может затрагивать

коммерческие интересы организации, но главной задачей имеет

обеспечение интересов клиентов либо собственных интересов,

непосредственно не связанных с коммерческой деятельностью.

Так, к служебной, а не к коммерческой, тайне следует отнести

сведения, касающиеся мер по обеспечению безопасности сотрудников организации, охране складских и иных помещений и

др., прямо не связанные с осуществлением предметной деятельности.

В настоящее время институт служебной тайны в отечественном праве является наименее разработанным. В этой проблеме можно выделить три ряда вопросов.

Во-первых, на законодательном уровне требуют урегулирования вопросы «пограничных» и «производных» сведений.

«Пограничные» сведения - это такая служебная информация в

любой отрасли науки, техники, производства и управления, которая при определенном обобщении и интеграции становится

государственной тайной. «Производные» сведения - служебная

информация, полученная в результате дробления сведений, составляющих государственную тайну, на отдельные компоненты,

каждый из которых не может быть к ней отнесен.

Во-вторых, особого правового регулирования требует защита сведений, образующихся в деятельности органов государственной власти и управления. Для формирования административно-правового института служебной тайны следует принять

специальный закон, действие которого должно распространяться на все уровни системы государственного управления.

В-третьих, требует защиты определенная категория значимых сведений субъектов гражданско-правовых отношений.

Здесь имеется в виду правовая защита сведений, которые в деятельности организаций не могут быть отнесены к коммерческой

тайне, несмотря на то, что в ГК РФ понятие служебной тайны

напрямую связано с действительной или потенциальной коммерческой ценностью информации.

Следует заметить, что в настоящее время практикуется упрощенный подход: любые сведения о предпринимательской

деятельности организации, доступ к которым ограничен, относят к коммерческой тайне. Однако при таком подходе могут

возникнуть трудности определения материального ущерба и

упущенной выгоды при неправомерном распространении конфиденциальной информации, например сведений о режиме охраны организации или других аспектах её функционирования,

напрямую не связанных с осуществлением предметной деятельности. Вместе с тем указанные сведения необходимо защищать,

т.к. от ограничения доступа к ним в значительной степени зависит коммерческий успех организации.

Профессиональные тайны

В соответствии с действующим законодательством к профессиональной тайне относится информация, связанная со служебной деятельностью медицинских работников, нотариусов,

адвокатов, частных детективов, священнослужителей, работников банков, ЗАГСов, учреждений страхования. В качестве субъекта профессиональной тайны может выступать как юридическое, так и физическое лицо.

Профессиональная тайна - информация, защита которой от несанкционированного распространения является обязанностью субъекта в силу выполняемых им

профессиональных функций._____ Сохранение в тайне сведений, полученных в связи с выполнением профессиональных функций, вызвано в первую очередь нормами профессиональной этики, а не собственными

коммерческими интересами предпринимателя или организации.

Соответствующий правовой статус рассматриваемым нормам

придает их законодательное закрепление.

1) банковская тайна. Понятие банковской тайны, в соответствии со ст. 857 ГК РФ, охватывает сведения о банковском

счёте, вкладе, операциях по счёту, а также сведения о клиентах

банка.

Банковская тайна защищает конфиденциальную информацию клиента или коммерческую информацию корреспондента.

ФЗ «О банках и банковской деятельности» определяет обязанности субъектов, категории информации и основания, по которым сведения предоставляются заинтересованным органам

государственной власти, организациям и лицам. Кредитная организация, Банк России гарантируют тайну об операциях, о счётах и вкладах своих клиентов и корреспондентов. Все служащие

кредитной организации обязаны хранить тайну об операциях,

счётах и вкладах её клиентов и корреспондентов, а также об

иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из

отчетов кредитных организаций, полученные им в результате

исполнения лицензионных, надзорных и контрольных функций,

за исключением случаев, предусмотренных федеральными законами.

Таким образом, кредитная организация вправе относить к

банковской тайне любые сведения, за исключением прямо указанных в Законе.

2) нотариальная тайна. Тайна является специфическим

правилом нотариальных действий. В соответствии со ст. 5 Основ законодательства РФ о нотариате нотариусу при исполнении служебных обязанностей, а также лицам, работающим в

нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения

полномочий или увольнения, за исключением случаев, предусмотренных Основами. Обязанность хранить профессиональную тайну включена в текст присяги нотариуса.

3) процессуальные тайны обычно делят на два вида:

следственную тайну и тайну совещания судей.

Следственная тайна связана с интересами законного производства предварительного расследования по уголовным делам

(ст. 31О УК РФ «Разглашение данных предварительного расследования»). Сведения о ходе предварительного расследования

могут быть преданы гласности только с разрешения прокурора,

следователя или лица, производящего дознание. Такая информация может касаться как характера производимых следственных действий, так и доказательственной базы, перспектив расследования, круга лиц, участвующих в расследовании. Важно

отметить, что законодательно не закреплен перечень сведений,

составляющих следственную тайну. Это означает, что прокурор,

следователь или лицо, производящее дознание, могут по своему

усмотрению устанавливать, какая информация о предварительном

расследовании может быть специально охраняемой, а какая - нет.

Тайна совещания судей. Для всех четырех видов существующих в отечественном судопроизводстве процессов предусмотрена определенная процедура обеспечения независимости и

объективности вынесения решения по делу. Эта процедура имеет одной из целей запрет на разглашение информации о дискуссиях, суждениях, результатах голосования, которые имели место

во время совещания судей. Обеспечение тайны совещания судей

устанавливается ст. 193 Гражданским Процессуальным Кодексом (ГПК) РФ, ст. 70 Федерального конституционного закона

«О Конституционном суде Российской Федерации», ст. 124 Арбитражного процессуального кодекса Российской Федерации.

4) врачебная тайна. Согласно ст. 61 Основ законодательства РФ об охране здоровья граждан информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные

при его обследовании и лечении, составляют врачебную тайну.

Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений.

5) адвокатская тайна. В соответствии с ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» адвокат, помощник адвоката и стажер адвоката не вправе разглашать

сведения, сообщенные доверителем в связи с оказанием ему

юридической помощи. Причем доверительные сведения, полученные адвокатом, могут быть как в виде документов, так и в

устном виде. Законом установлены гарантии независимости адвоката. В частности, адвокат не может быть допрошен в качестве свидетеля об обстоятельствах, которые стали ему известны в

связи с исполнением им обязанностей защитника или представителя (ст. 15 указанного Закона).

6) тайна страхования. Институт страховой тайны во многих отношениях схож с институтом банковской тайны. Тайну

страхования, в соответствии со ст. 946 ГК РФ, составляют полученные страховщиком в результате своей профессиональной

деятельности сведения о страхователе, застрахованном лице и

выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и

характера нарушения несет ответственность в соответствии с

правилами, предусмотренными ст. 139 или ст. 150 ГК РФ.

Согласно ст. 8 Закона РФ «Об организации страхового дела в Российской Федерации» в качестве лица, обязанного сохранять тайну страхования, могут выступать как юридические, так

и физические лица - страховые агенты и страховые брокеры.

Кроме того, в соответствии со ст. 33 указанного Закона должностные лица федерального органа исполнительной власти по

надзору за страховой деятельностью не вправе использовать в

корыстных целях и разглашать в какой-либо форме сведения,

составляющие коммерческую тайну страховщика.

7) тайна связи. ФЗ «О связи» в части защиты информации

регулирует общественные отношения, связанные с обеспечением невозможности противоправного ознакомления с сообщениями, передаваемыми любыми субъектами - физическими или

юридическими лицами - по средствам связи. При такой постановке вопроса тайна связи становится инструментом обеспечения сохранности конфиденциальной информации.

Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по

сетям электрической и почтовой связи, охраняется Конституцией РФ. Обязанность обеспечения соблюдения тайны связи возлагается на оператора связи, под которым понимается физическое или юридическое лицо, имеющее право на предоставление

услуг электрической или почтовой связи. Также операторы связи обязаны соблюдать конфиденциальность сведений об абонентах и оказываемых им услугах связи, ставших известными операторам в силу выполнения профессиональных обязанностей.

8) тайна усыновления. Институт тайны усыновления связан с интересами охраны семейной жизни и выражается в установлении гражданской и уголовной ответственности за разглашение тайны усыновления (удочерения). Согласно ст. 155 УК

РФ тайна усыновления может быть двух разновидностей. Первой обладают лица, которые обязаны хранить факт усыновления

как служебную или профессиональную тайну (судьи, работники

местных администраций, органов опеки и попечительства и

прочие лица, указанные в ч. 1 ст. 139 СК РФ). Второй - все другие лица, если установлены их корыстные или иные низменные

побуждения при разглашении тайны усыновления без согласия

обоих усыновителей.

9) тайна исповеди. Обеспечение тайны исповеди является

внутренним делом священника; юридической ответственности

за её разглашение он не несет. Согласно ч. 2 ст. 51 Конституции

РФ и ч. 7 ст. 3 ФЗ «О свободе совести и религиозных объединениях» священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали ему известны из исповеди.

Персональные данные

В соответствии с ФЗ «О персональных данных» от 27 июля

2006 года № 152 определен круг сведений, которые могут быть

отнесены к персональным данным.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании

такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация._____

В России нормы, регулирующие вопросы защиты персональных данных, были впервые включены в Конституцию РФ

1993 г. Согласно ст. 23 и 24 Конституции РФ каждый гражданин

РФ имеет право на неприкосновенность частной жизни, личную

и семейную тайну, защиту своей чести и доброго имени. Сбор,

хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому

возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное

не предусмотрено законом.

Конституционное положение о недопустимости сбора,

хранения, использования и распространения информации о частной жизни лица является одной из гарантий закрепленного в

ст. 23 Конституции РФ права на неприкосновенность частной

жизни. Оно призвано защитить частную жизнь, личную и семейную тайну от какого бы то ни было проникновения в неё со

стороны как государственных органов, органов местного самоуправления, так и негосударственных предприятий, учреждений, организаций, а также отдельных граждан. В соответствии с

ФЗ «Об информации, информационных технологиях и о защите

информации» запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в

том числе информации, составляющей личную или семейную

тайну, и получать такую информацию помимо воли гражданина

(физического лица), если иное не предусмотрено федеральными

законами.

Особое значение запрет собирать, хранить, использовать

и распространять информацию о частной жизни лица приобретает

в связи с созданием информационных систем на основе использования средств вычислительной техники и связи, позволяющих

накапливать и определенным образом обрабатывать значительные

массивы информации. Порядок доступа к персональным данным

граждан (физических лиц) устанавливается ФЗ «О персональных

данных». В Уголовном кодексе РФ существуют ст. 137 и 140, устанавливающие ответственность за нарушение неприкосновенности

частной жизни.

Защита интеллектуальной собственности

Международное право в сфере защиты информации

Защита авторских и смежных прав в законодательстве РФ

Объекты авторского права

Субъекты авторского права

Права обладателей авторских прав

Международное право в сфере защиты информации

До середины XIX в. авторское право как таковое не существовало. Право собственности могло распространяться лишь на конкретные овеществленные произведения искусства (картины, скульптуры и т.п.). Начиная с середины XIX в. авторское право становится самостоятельной формой собственности - произведения интеллектуального труда стали отвечать всем признакам товара.

Бернская конвенция «Об охране литературных и художественных произведений» (1886 г.). Работа по созданию правового инструмента по охране авторского права была начата в Брюсселе в 1858 г. на состоявшемся там конгрессе авторов произведений литературы и искусства. Затем последовали конгрессы в Антверпене (1861 и 1877 г.) и Париже (1878 г.), с 1883 г. работа была продолжена в Берне, где в 1886 г. после трех дипломатических конференций было выработано международное соглашение, получившее название Бернской конвенции об охране литературных и художественных произведений. Соглашение было подписано девятью государствами: Бельгией, Великобританией, Испанией, Италией, Либерией, Гаити, Тунисом, Францией и Швейцарией. Конвенция вступила в силу 5 декабря 1887 г.

Основные положения Конвенции подлежали обязательному включению в национальные законодательства стран участниц в тех случаях, когда национальные законодательства
обеспечивали менее благоприятный режим для обладателей авторских прав. В этом проявилось стремление создателей Конвенции к унификации основных положений авторского права.

Парижская конференция (1896 г.). 15 апреля 1896 г. в Париже состоялась первая конференция по изменению Конвенции
1886 г. В конвенцию было включено понятие «публикация»,
определенное как выпуск копий. Таким образом, представление
и исполнение драматических, драматическо-музыкальных и музыкальных произведений, выставки произведений искусства к публикации не относились. Было также принято уточнение к ст. 3,
в соответствии с которым охрана предоставлялась произведению,
впервые опубликованному в стране-участнице Конвенции даже
в том случае, когда автор был гражданином страны, не входящей
в Бернский союз. Территориальный принцип Конвенции оставался
неизменным, однако акцент был перенесен с издателя на автора
произведения.

Берлинская конференция (1908 г.). Результатом работы
конференции явился почти полный пересмотр всех основных
положений Бернской конвенции. Новая редакция содержала 30
статей, и основные нововведения относились к следующим проблемам.

Конвенция 1886 г. ставила охрану авторского права в зависимость от условий выполнения формальностей, предусмотренных в стране первой публикации. На Берлинской конференции было решено отказаться от всех формальностей даже в том
случае, если в стране первой публикации они существуют.

Берлинский вариант Конвенции более полно определил и
существенно расширил круг объектов охраны, включив в него

произведения хореографии и пантомимы, кинематографии, фотографии и архитектуры. Были признаны права композиторов на
разрешение адаптировать их произведения для исполнения аппаратами механического воспроизведения и их публичное исполнение.
Правила, регламентирующие право перевода, были расширены. Берлинская конференция признала их действительность на протяжении всего срока действия авторского права без
всяких ограничений.
Срок охраны авторского права был установлен равным 50
годам, исчисляемым со дня смерти автора. Правило не носило
обязательный характер - допускались различия в сроках охраны
авторских прав, определяемые законом страны, где ищется защита.
Конвенция более четко определила понятия литературного и художественного произведений и закрепила положение
о том, что они должны охраняться во всех странах-участницах
с обязательным отражением этого в национальных законодательствах.
Римская конференция (1928 г.). Римская конференция
проходила в период бурного развития средств массовой информации и коммуникаций. Это нашло отражение в признании охраны прав авторов при трансляции по радио их произведений, в
расширении числа объектов охраны, признании личных прав
автора и т.п.
Уровень охраны авторского права был повышен в связи с
включением в число объектов авторского права устных литературных произведений (лекций, речей, проповедей и т.п.). К числу наиболее важных нововведений следует отнести признание
так называемых личных прав автора, которые сохраняются за
ним и при отчуждении имущественных прав (издание, публикация, постановка и т.п.).
Брюссельская конференция (1948 г.). Бернская конвенция

подверглась существенным изменениям в Брюсселе в 1948 г.

Основной целью конференции было стремление добиться более полной унификации правил Конвенции и национальных законодательств, а также учесть новые условия научного и технического развития. Унификация правил применения Конвенции была достигнута путем усиления принципа её главенства над национальными законодательствами.

Всемирная конвенция об авторском праве (1952 г.). Говоря о причинах принятия Всемирной конвенции об авторском праве, следует иметь в виду прежде всего стремление к этому Соединенных Штатов Америки и ряда других стран, которые хотели иметь соглашение с как можно меньшим количеством императивных условий и формальностей. Всемирная конвенция об авторском праве была принята на состоявшейся в Женеве в сентябре 1952 г. межправительственной конференции с участием представителей 50 стран. Конвенция вступила в силу в сентябре 1955 г.

Женевская конвенция об авторском праве содержит общую декларацию о стремлении стран-уЧастниц конференции создать международно-правовой инструмент, приемлемый для возможно более широкого крута стран и направленный на облегчение распространения произведений интеллектуального творчества в целях лучшего международного взаимопонимания.

Стокгольмская конференция (1967 г.). К этому времени на международной арене появилось большое количество развивающихся стран с их специфическими нуждами и проблемами, которые стремились понизить уровень охраны авторских прав с целью получения свободного доступа к произведениям науки и культуры. Добившиеся высокого уровня охраны авторских прав, развитые капиталистические страны боялись наметившейся

тенденции и всячески ей противились. Для сохранения прежнего уровня охраны авторского права предполагалось пойти на
сужение границ Бернского союза. Россия присоединилась к
Бернской конвенции лишь спустя почти 100 лет после её первого опубликования, в ноябре 1994 г.
Постановлением Правительства РФ от 3 ноября 1994 г.
№1224 Российская Федерация присоединилась к Бернской конвенции об охране литературных и художественных произведений в редакции 1971 г. и Всемирной конвенции об авторском
праве в редакции 1971 г.
Защита авторских и смежных прав в законодательстве РФ
В настоящее время положение с охраной и защитой прав
на интеллектуальную собственность в России характеризуется
как весьма тревожное.
Высокая доходность и доступность интеллектуальной
собственности стала особенно привлекательной для дельцов
«теневой» экономики. Преступность в данной сфере приняла
устойчивые организационные формы. Налажены нелегальные
каналы быстрого получения экземпляров новых программных
продуктов, их взлома в случаях, когда они защищены ключами
аппаратной защиты или программными средствами, а также получения новинок аудио-видеопродукции, организованы подпольные технологические линии по тиражированию носителей программ для ЭВМ и аудио-видеокассет, установлены криминальные
связи с легальными заводами-производителями компьютерных
носителей (компакт-дисков) и по изготовлению крупных партий
контрафактного программного обеспечения, аудио-видеопродукции
и производству дополнительных (официально не учтенных) тиражей легальной продукции без ведома правообладателя, созданы
и действуют оптовые и розничные сбытовые сети.

В отличие от темпов развития законодательства, защищающего авторские права на объекты интеллектуальной собственности, организованная преступность в этой сфере развивается довольно стремительно. Этому способствуют: извлечение из данной деятельности крупной прибыли при минимальных издержках; коррумпированные связи дельцов в государственных органах, в том числе и правоохранительных; несовершенство законодательства и низкий уровень правосознания общества.

Интеллектуальной собственность - совокупность исключительных прав на результаты интеллектуальной деятельности, а также на некоторые иные приравненные к ним объекты, такие как средства индивидуализации участников гражданского оборота и производимой ими продукции (работ, услуг)._____

Понятие «интеллектуальная собственность» включает в себя не только авторские права и права на промышленную собственность, но и права на средства индивидуализации товаров и услуг. Кроме этого, имеются специальные законы о специфичных объектах интеллектуальной собственности - топологии интегральных микросхем и селекционных достижениях.

В юридической литературе существуют и другие мнения о понятии «интеллектуальная собственность». Под интеллектуальной собственностью иногда понимают нематериальные объекты авторского и патентного права, иногда их ещё называют «промышленная собственность» или «литературная собственность». Однако произведение (изобретение, товарный знак, фирменное наименование и т.д.), охраняемое авторским и патентным правом, имеет такие особенности духовного порядка, которые не позволяют отождествить его с вещью. Материальное воплощение идей и образов представляет собой «вещь» настолько условную, что по отношению к праву на объект любого

творческого произведения правильнее применять термин «интеллектуальные права».

Авторское и патентное права, специфическим объектом которых как раз и является творческое произведение, регулируют данные отношения настолько своеобразно, что становится невозможным даже проведение аналогий между нормами о праве собственности и нормами об интеллектуальных правах. Однако следует отметить, что правовой режим охраны нематериальных объектов выполняет в отношении нематериальных объектов ту же функцию, что и право собственности в отношении материальных объектов (вещей), устанавливает абсолютное право, дающее возможность субъекту (обладателю права) вводить объект в хозяйственный оборот.

Понятие «право собственности» в объективном смысле представляет собой совокупность правовых норм, регулирующих отношения собственности в данном обществе и действительных для всех членов общества, а нарушение этих норм влечет за собой применение принудительных санкций государства.

Право интеллектуальной собственности не является разновидностью права собственности. Это два различных правовых института. Под интеллектуальной собственностью понимаются исключительные права на результаты интеллектуальной деятельности, т.е. на нематериальные объекты, тогда как право собственности относится к вещным правам.

В целях обеспечения защиты авторских, издательских, иных прав на интеллектуальную собственность с 1 января 2008 года вступил в силу раздел VII «Права на результаты интеллектуальной деятельности и средства индивидуализации» ГК РФ от 18 декабря 2006 г. № 230-ФЭ (часть четвертая).

Защита прав на результаты интеллектуальной деятельности осуществляется в судебном (общем) и административном

(специальном, применяемом в прямо указанных законом случаях) порядке.

Конституция РФ гарантирует каждому свободу литературного, научного, технического и других видов творчества, при

этом подчеркивается, что интеллектуальная собственность охраняется законом. Одной из гарантий реализации авторских и

смежных прав, декларированной ст. 44 Конституции РФ, является уголовно-правовая защита этих прав, установленная ст. 146

УК РФ.

Действующий УК РФ предусматривает уголовную ответственность за преступления в сфере интеллектуальной собственности по ст. 146 «Нарушение авторских и смежных прав», ст.

147 «Нарушение изобретательских и патентных прав», ст. 180

«Незаконное использование товарного знака».

Правоприменительная практика российского законодательства, защищающего объекты интеллектуальной собственности, окончательно ещё не сложилась. Но в целом борьба с преступлениями в сфере интеллектуальной собственности в ближайшем будущем приобретет ещё большую актуальность, т.к. с

каждым днем возрастает значимость объектов интеллектуальной собственности, что обусловлено требованиями научнотехнического прогресса, экономическим и социальным развитием России.

Объекты авторского права

Авторское право и регулируемые им имущественные и личные неимущественные отношения связаны с созданием и использованием произведений литературы, науки и искусства. Авторское

право как самостоятельный институт решает конкретные задачи,

которые включают:

- всемерную охрану имущественных, личных неимущественных прав и законных интересов авторов;

- обеспечение правовыми средствами наиболее благоприятных условий для создания научных и художественных произведений;

- широкое использование их обществом.

Международное авторское право является частью международного частного права. В первоначальном тексте Бернской конвенции 1886 г. понятие «литературные и художественные произведения» было определено через перечисление различных конкретных видов произведений (книги, брошюры, картины и т.п.). Здесь же говорилось о произведениях в области литературы, науки и искусства, которые могут быть выпущены в свет «любым способом издания или воспроизведения». На сегодняшний день круг произведений намного расширился.

Можно выделить ряд основных объектов авторского права.

Литературные произведения составляют значительную часть объектов авторского права. Особенность их в том, что мысли, чувства, идеи и образы выражаются посредством слова в оригинальной композиции и оригинальном изложении.

В структуре литературного произведения выделяются тема, материал, идеология, образная система, сюжет, язык, заглавие. Эти элементы литературного произведения разделяются на юридически безразличные, т.е. тема, материал, сюжет, идейное содержание, и юридически значимые - образная система и язык.

Использование значимых элементов произведения в ряде случаев требует согласия автора.

Литературная обработка - особый объект авторского права. Она представляет собой музыкальную или литературную обработку произведений авторов, которые в силу некоторых причин (отсутствие навыков и др.) не в состоянии сами привести свое произведение в законченный вид. Кроме того, обработке могут подвергаться народные произведения, произведения неизвестных авторов и т.д. Записанный и обработанный литературный материал должен отвечать требованиям, предъявляемым

законом к литературным и музыкальным произведениям.

Музыкальные произведения выражаются в сочетании
звуков, образующих мелодию и связанных ритмом и гармонией.

Они имеют форму ораторий, симфоний, песен и т.п. Кроме музыкальных произведений существуют также музыкальнодраматические произведения, которые создаются на литературнодраматической основе (либретто) и исполняются на сцене в виде
опер, балетов, оперетт.

Музыкальные произведения записываются композитором
особыми знаками, позволяющими фиксировать его творческий
замысел. Нотная запись музыкального произведения образует
клавир, представляющий собой переложение музыкального
произведения для фортепиано, или же партитуру, содержащую
все партии многоголосного музыкального произведения. Музы-
кальное произведение может фиксироваться также на аудионосителях (кассеты, компакт-диски и т.п.).

Обработка чужих произведений, оркестровка, переложение относятся к объектам авторского права, если они содержат
элемент творчества.

Хореографические произведения, или пантомимы, -
произведения искусства, создаваемые при помощи пластических
движений человеческого тела. В сочетании с музыкой хореографическое произведение образует музыкально-сценическое
произведение. В связи с тем, что хореографические произведения довольно сложно закрепить с помощью каких-то особых
знаков на бумаге, для этих целей, как правило, используют фото», кино- и видеозапись.

Произведения изобразительного искусства - это произведения живописи, графики, скульптуры, декоративноприкладного искусства и т.п. Художники, скульпторы создают

оригинальные произведения, которые могут воспроизводиться путем изготовления копий либо самими авторами, либо иными лицами.

Архитектурные произведения (проекты) также являются объектами авторского права. Они представляют собой синтез инженерного искусства, бионики, живописи, скульптуры, науки, архитектуры. В них слиты наука, техника, искусство. Эскизный архитектурный проект, в котором воплощается замысел автора, содержит решения будущего произведения, внутреннее развитие его сочлененных пространств, их объёмы, фактуру и цвет.

На основе эскизного архитектурного проекта строятся здания, сооружения, комплексы и т.п.

Аудиовизуальные произведения - достаточно широкая категория, охватывающая многообразные произведения для кино, телевидения, радио, интерактивных сетей и т.п.: сценарии, сценарные планы, тексты песен, кинофильмы, телепередачи, радиопередачи, заставки и многое другое. Данная категория произведений, как правило, закрепляется на аудио-, кино- и видеоносителях (пленка, кассеты, цифровые носители и т.п.).

Программные продукты для средств вычислительной техники могут представлять собой как отдельные прикладные программы (текстовые редакторы, компиляторы и т.п.), так и базы данных, энциклопедии, мультимедийные программы. Кроме того, особенность этой категории заключается в том, что в программах для ЭВМ может иметь место использование других объектов авторского права, это могут быть произведения литературы, музыкальные произведения, произведения изобразительного искусства, кинематографии, а также многое другое. В связи со стремительным прогрессом в области использования

вычислительной техники закономерно ожидать появления новых норм внутригосударственного и международного права, направленных на разрешение множества коллизий.

Все вышеперечисленные объекты авторского права можно отнести к категории оригинальных произведений, создаваемых авторами. Кроме них конвенционной охране подлежат также зависимые произведения, возникшие на основе существующих оригинальных произведений. Эти произведения появляются в результате перевода (с иностранного языка), переделки, составительства.

Зависимость перевода литературного, художественного, научного произведения от оригинала не лишает его самостоятельности. Конвенция относит переводы к объектам авторского права, сохраняя для них те же критерии охраноспособности, что и для других произведений. Если же переводчик ограничивает свою работу лишь подбором равнозначных слов к языку оригинала, то подобный перевод («подстрочник») не может быть объектом авторского права. Перевод, выполненный с согласия автора или его правопреемников одним лицом, не может препятствовать другому лицу осуществлять новый перевод этого же произведения.

К объектам авторского права относятся сборники произведений. В сборники могут включаться произведения, не являющиеся предметом чьего-либо авторского труда (законы, статистика, судебные решения и т.д.), а также произведения отдельных авторов.

Творческий характер труда составителя заключается в подборе и расположении материала. Авторское право составителя сборника не может мешать другому лицу самостоятельно систематизировать, обрабатывать и выпускать в свет те же произведения.

Научное произведение - это определенная система понятий. Научное произведение может быть выражено в форме учебника, монографии, статьи и т.д. Существуют и другие фор-

мы воплощения научных произведений: чертежи, планы, эскизы, модели, компьютерные программы, различного рода карты и т.п.

Основное отличие авторского права от режима правовой охраны других результатов интеллектуальной деятельности состоит в том, что произведение литературы, науки и искусства становится объектом авторского права в силу самого факта его создания автором без какой-либо регистрации, оформления или соблюдения иных формальностей.

Субъекты авторского права

Субъектами авторского права выступают лица, создавшие творческим трудом произведения литературы, науки и искусства (авторы). Возникновение субъективных авторских прав у гражданина не зависит от возраста, имущественного положения, места создания и выпуска произведения в свет и т.п. Субъектом авторских прав может стать даже человек, признанный судом недееспособным (например, по причине душевной болезни).

Иностранный гражданин может быть субъектом российского авторского права, если его произведение впервые выпушено в свет на территории страны либо не выпущено, но находится на её территории в какой-либо объективной форме. Когда произведение иностранного автора впервые выпущено в свет за границей или находится там в объективной форме, этот автор становится субъектом российского авторского права только в силу заключенных РФ соглашений и в пределах, ими установленных.

Наряду с авторами произведений к субъектам авторского права относятся лица (граждане и организации), которые не участвуют в творческом создании произведений литературы, науки и искусства. Их называют правопреемниками. К правопреемникам переходит определенный круг авторских правомочий по использованию произведений автора, основанием такого перехода служит закон, наследование или договор с автором.

Как правило, автором того или иного произведения выступает одно лицо, которое создало его творческим трудом. Однако в работе над произведением литературы, науки и искусства
могут быть объединены усилия нескольких лиц - соавторов.
Особое место в международной системе охраны авторских
прав занимают обладатели так называемых смежных прав. Это
новое понятие для нашего права, а в некоторых странах понятие
«обладатели смежных прав» вообще не используется. К такого
рода субъектам относится достаточно широкий круг лиц, таких
как режиссеры, актеры, исполнители, продюсеры и т.п.
В международном праве охрана прав, примыкающих к авторским, осуществляется в соответствии с международной конвенцией об охране прав артистов, исполнителей, изготовителей
фонограмм и вещательных организаций, подписанной в Риме в
1961 г. Эта Конвенция представляет собой попытку сбалансировать охрану всех категорий субъектов авторского права.
Права обладателей авторских прав
Автором произведения признается гражданин, творческим
трудом которого оно создано.
Автору произведения принадлежит исключительное право
на свое произведение, включающее:
- право авторства;
- право на имя;
- право на неприкосновенность произведения;
- право на опубликование произведения;
- право на использование произведения (право осуществлять или разрешать его воспроизведение любыми способами - в
печати, путем публичного исполнения, передачи в эфир, в видео- и звукозаписи, по кабельному телевидению, с помощью
спутников и иных технических средств; перевод, переработку

произведения; распространение экземпляров воспроизведенного произведения; реализацию архитектурного и дизайнерского проекта и т.п.);

- право на вознаграждение за разрешение использовать и использование произведения.

Автор может передать право на использование своего произведения как на территории своего государства, так и за рубежом любым гражданам и юридическим лицам, в том числе и иностранным.

Авторское право на произведение, созданное совместным творческим трудом двух или более граждан, принадлежит соавторам совместно, независимо от того, образует ли такое произведение одно неразрывное целое или состоит из частей, каждая из которых имеет также самостоятельное значение.

Взаимоотношения соавторов могут определяться договором между ними. Каждый из соавторов сохраняет авторское право на созданную им часть произведения, имеющую самостоятельное значение, и вправе использовать такую часть произведения по своему усмотрению.

Составители сборников произведений, которые представляют собой по подбору и расположению материалов результат творческого труда, пользуются авторским правом на сборник при условии соблюдения прав авторов каждого из произведений, включенных в сборник.

Авторы произведений, включенных в сборник, сохраняют авторское право каждый на свое произведение и могут использовать свои произведения независимо от сборника в целом.

Организации, выпускающие в свет энциклопедии, энциклопедические словари, газеты, журналы, периодические и продолжаемые сборники научных трудов и другие периодические издания, пользуются правом на использование издания в целом,

если иное не установлено в договорах с авторами, произведения которых включены в такое издание.

Авторы кино-, теле- и видеофильма по авторским договорам передают право на использование фильма его изготовителю в пределах, предусмотренных договором.

Авторы произведений, использованных в фильме, сохраняют авторское право каждый на свое произведение, передают изготовителю право на его использование и могут использовать произведение независимо от фильма в целом.

К наследникам автора переходит право охраны неприкосновенности произведения, право осуществлять или разрешать его опубликование или использование, а также право на получение вознаграждения за разрешение использовать или использование произведения.

К иным правопреемникам автора, в том числе юридическим лицам, может переходить только право ка использование произведения.

Обладатели «смежных прав» имеют следующие права:

исполнителям-артистам, режиссерам-постановщикам и дирижерам принадлежат право на имя, право на защиту постановки и исполнения произведения, право осуществлять или разрешать использование постановки и исполнения и право на вознаграждение. Запись исполнения, трансляция и иное использование могут производиться только с согласия исполнителя.

Лицу, создавшему звуко- и видеозапись, принадлежит право осуществлять или разрешать её воспроизведение. Использование звуко- и видеозаписи допускается только с разрешения этого лица или его правопреемника (правообладателя).

Право на звуко- и видеозапись включает право её воспроизведения любыми способами, право её публичного распространения, в том числе передачи за границу, а также право на
защиту от импорта и распространения экземпляров записи без
разрешения правообладателя. Если право собственности на экземпляр звуко- или видеозаписи принадлежит не её создателю,
то исключительное право коммерческого проката сохраняется за
лицом, создавшим звуко- или видеозапись.

Организациям эфирного вещания принадлежит право разрешать другим организациям ретрансляцию, запись и воспроизведение их передач. Организациям публичного вещания принадлежит также право разрешать публичное воспроизведение
телевизионных передач, если оно производится за плату в местах, доступных неопределенному кругу лиц.

Создатели звуко- и видеозаписей, организации эфирного
вещания осуществляют свои права в пределах прав, полученных
по договору с автором и исполнителем, а организации эфирного
вещания так же, без ущерба правам создателей звукозаписи.

Исполнители осуществляют свои права с соблюдением
прав авторов исполняемых ими произведений.

Чтобы защитить своё исключительное право на использование программного продукта, правообладатель может обратиться в суд, арбитражный или третейский суд и требовать возмещения причиненных убытков, в размер которых включается
сумма доходов, неправомерно полученных нарушителем, или
выплаты нарушителем компенсации, определяемой по усмотрению судебных органов. Помимо возмещёния убытков или выплаты компенсации по усмотрению судебного органа в доход
бюджета России может быть взыскан штраф в размере 10%
суммы, присужденной в пользу истца.

Судебный орган может вынести решение о конфискации

контрафактных экземпляров программного продукта, а также материалов и оборудования, используемых для их воспроизведения, и об их уничтожении либо о передаче их в доход бюджета Российской Федерации, либо истцу по его просьбе в счёт возмещёния убытков.

Тем не менее в настоящее время существующую судебную практику защиты прав правообладателя нельзя, к сожалению, считать совершенной; имеющиеся случаи судебной защиты авторских прав пока ещё редки, однако ситуация меняется - ещё несколько лет назад в судах подобные дела к производству практически не принимались.

5. Защита государственной тайны

Государственная тайна как особый вид защищаемой информации
Ущерб от утечки сведений, составляющих государственную тайну
Система защиты государственной тайны
Способы защиты государственной тайны
Режим секретности

Государственная тайна как особый вид защищаемой информации

В современном мире информация рассматривается как один из наиболее ценных продуктов человеческой жизнедеятельности, а информационные ресурсы и технологии, которыми располагает государство, определяют его стратегический потенциал и влияние в мире. В результате безопасность государства, его общественно-политических институтов, организаций и граждан включает в настоящее время в качестве обязательной составляющей информационную безопасность. Важным элементом информационных ресурсов является государственная тайна, отнесенная по условиям правового режима к документированной информации ограниченного распространения.

Тайны являются неотъемлемой составляющей общественной жизни, частью правовой системы и могут служить даже своеобразным мерилом для определения вида политического режима в государстве, ибо состояние защиты секретов отражает характер взаимоотношений общества и государства, демократизации государственной власти.

Государственные средства воздействия на информационные процессы - важнейшее политическое условие обеспечения прав человека и рационализации использования информационных ресурсов в обществе. Система защиты секретов - наиболее сильное звено государственного опосредования общественных отношений в информационной сфере. Сведения, составляющие государственную тайну, имеют особую важность для общества и государства.

Вследствие величины возможного ущерба от её разглашения государственная тайна занимает приоритетное место в системе социального института тайн. Режим защиты государственной тайны - важнейший элемент системы государственного управления.

Правовой институт государственной тайны - признанный всеми странами институт регулирования информационных общественных отношений. Государственная секретность в той или иной степени наличествует во всех государствах мира. Это вполне объяснимо и логично, поскольку информация, с одной стороны - объект отношений людей, а с другой - ресурс: ресурс управления, принятия решений. Поэтому в качестве реальной угрозы своей безопасности государства рассматривают потенциально возможную утечку защищаемой информации за границу.

Правовой институт государственной тайны имеет три составляющие:

1) сведения, относимые к определенному типу тайны (а также принципы и критерии, по которым сведения классифицируются как тайна);

2) режим секретности (конфиденциальности) - механизм ограничения доступа к указанным сведениям, т.е. механизм их защиты;

3) санкции за неправомерное получение и (или) распространение этих сведений.

Понятие «государственная тайна» является одним из важнейших в системе защиты государственных секретов в любой

стране. От её правильного определения зависит и политика руководства страны в области защиты секретов. Определение этого понятия дано в Законе РФ «О государственной тайне».

Государственная тайна - защищаемые государством

сведения в области его военной, внешнеполитической,

экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации._____

В этом определении указываются категории сведений, которые защищаются государством, и сообщается, что распространение этих сведений может нанести ущерб интересам государственной безопасности. Для сравнения приведем краткие

определения понятия «государственная тайна», даваемые специалистами других стран.

В Уголовном кодексе ФРГ зафиксировано, что государственной тайной являются факты, предметы или познания, которые доступны лишь ограниченному кругу лиц и должны содержаться в тайне от иностранного правительства, чтобы предотвратить опасность наступления тяжкого ущерба для внешней

безопасности ФРГ.

В Исполнительном Указе Президента США от 2.04.1982 г.

говорится, что к информации по национальной безопасности

относится определенная информация по национальной обороне

и международным вопросам, которая защищается от несанкционированного раскрытия.

В некоторых странах это понятие выражается в других

терминах, например, в Японии - «оборонный секрет».

Модель определения государственных секретов обычно

включает в себя следующие существенные признаки:

1) предметы, явления, события, области деятельности, составляющие государственную тайну;

2) противник (данный или потенциальный), от которого в

основном осуществляется защита государственной тайны;

3) указание в законе, перечне или инструкции сведений,

составляющих государственную тайну;

4) наносимый ущерб обороне, внешней политике, экономике, научно-техническому прогрессу страны и т.п. в случае

разглашения (утечки) сведений, составляющих государственную тайну.

Важным признаком государственной тайны является степень секретности сведений, отнесенных к ней. В нашей стране

принята следующая система обозначения сведений, составляющих государственную тайну: «особой важности», «совершенно

секретно», «секретно». Эти грифы проставляются на документах

или изделиях (их упаковках или сопроводительных документах). Содержащиеся под этими грифами сведения являются государственной тайной.

К сведениям особой важности (Правила отнесения сведений, составляющих государственную тайну, к различным степеням

секретности, приведены в Постановлении Правительства РФ от

4 сентября 1995 г. № 870) следует относить такие сведения, распространение которых может нанести ущерб интересам Российской

Федерации в одной или нескольких областях.

К совершенно секретным сведениям следует относить

такие сведения, распространение которых может нанести ущерб

интересам министерства (ведомства) или отраслям экономики

Российской Федерации в одной или нескольких областях.

К секретным сведениям следует относить все иные из

числа сведений, составляющих государственную тайну. Ущерб

может быть нанесен интересам предприятия, учреждения или
организации.

Перечень сведений, которые могут быть отнесены к государственной тайне, содержится в ст. 5 Закона РФ «О государственной тайне».

Государственную тайну составляют:

1) сведения в военной области:

- о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному
развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных
Федеральным законом «Об обороне», об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

- о планах строительства Вооруженных Сил Российской
Федерации, других войск Российской Федерации, о направлениях
развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских
и опытно-конструкторских работ по созданию и модернизации
образцов вооружения и военной техники;

- о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их
составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или)
методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

- о тактико-технических характеристиках и возможностях
боевого применения образцов вооружения и военной техники, о
свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

- о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

- о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и
(или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

- о содержании планов подготовки Российской Федерации
и её отдельных регионов к возможным военным действиям, о
мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и
материалов, а также о размещении, фактических размерах и об
использовании государственных материальных резервов;

- об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности
государства;

- о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности
населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

- об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой
оборонной продукции, о наличии и наращивании мощностей по
их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанного вооружения, военной техники и другой оборонной продукции;

- о достижениях науки и техники, о научно-исследовательских,

об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение,

влияющих на безопасность государства;

- об объемах запасов, добычи, передачи и потребления

платины, металлов платиновой группы, природных алмазов, а

также об объемах других стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

3) сведения в области внешней политики и экономики:

- о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

- о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней

задолженности), а также о финансовой или денежно-кредитной

деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

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

- о силах, средствах, об источниках, о методах, планах и

результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

- о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную

деятельность;

- об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также

данные о финансировании этой деятельности, если эти данные

раскрывают перечисленные сведения;

- о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о

шифрах, о разработке, об изготовлении шифров и обеспечении

ими, о методах и средствах анализа шифровальных средств и

средств специальной защиты, об информационно-аналитических

системах специального назначения;

- о методах и средствах защиты секретной информации;

- об организации и о фактическом состоянии защиты государственной тайны;

- о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального

шельфа Российской Федерации;

- о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;

- о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

В статье 7 Закона РФ «О государственной тайне» приведён перечень сведений, не подлежащих отнесению к государственной тайне и засекречиванию. Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях,

а также о стихийных бедствиях, их официальных прогнозах и

последствиях;

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

о состоянии преступности;

- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных

резервах Российской Федерации;

- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

Ущерб от утечки сведений, составляющих государственную тайну

Понятие, виды и размер ущерба разработаны пока ещё недостаточно и, видимо, будут различны для каждого конкретного

объекта защиты: содержания сведений, составляющих государственную тайну, сущности отраженных в ней фактов, событий,

явлений действительности. В зависимости от вида, содержания

и размеров ущерба можно выделить группы некоторых видов

ущерба при утечке (или возможной утечке) сведений, составляющих государственную тайну.

Политический ущерб может наступить при утечке сведений политического и внешнеполитического характера, о разведывательной деятельности спецслужб государства и др. Политический ущерб может выражаться в том, что в результате утечки информации могут произойти серьезные изменения в международной обстановке не в пользу Российской Федерации, утрата

страной политических приоритетов в каких-то областях, ухудшение отношений с какой-либо страной или группой стран и т.д.

Экономический ущерб может наступить при утечке сведений любого содержания: политического, экономического, военного, научно-технического и т.д. Экономический ущерб может

быть выражен прежде всего в денежном исчислении. Экономические потери от утечки информации могут быть прямые и косвенные.

Прямые потери могут наступить в результате утечки секретной информации о системах вооружения, обороны страны,

которые в результате этого практически потеряли или утратили

свою эффективность и требуют крупных затрат на их замену

или переналадку. Косвенные потери чаще всего выражаются в

виде размера упущенной выгоды: срыв переговоров с иностранными фирмами, о выгодных сделках с которыми ранее была договоренность; утрата приоритета в научном исследовании, в результате чего соперник быстрее довел свои исследования до завершения и запатентовал их и т.д.

Моральный ущерб, как правило, неимущественного характера, наступает от утечки информации, вызвавшей или инициировавшей противоправную государству пропагандистскую кампанию, подрывающую репутацию страны, приведшую к выдворению из каких-то государств наших дипломатов, разведчиков,

действовавших под дипломатическим прикрытием, й т.п.

Тенденция увеличения степени открытости государства

перед обществом диктует необходимость максимально возможного сокращения числа сведений, относимых к государственной

тайне, открытости общего перечня относимых к ней категорий

сведений, механизмов засекречивания и условий рассекречивания. Обязанность государства - взять на себя формирование

взвешенного механизма защиты различных видов информации и

установления рамок действия институтов тайн. Такие требования возникают из потребности современного общества быть более открытым и доступным, и диктуются необходимостью обеспечения безопасности личности, общества и государства.

Система защиты государственной тайны

В общем смысле защита информации - комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию

условий, ограничивающих её распространение и исключающих или существенно затрудняющих несанкционированный,

незаконный доступ к засекреченной информации и её носителям.

Защита информации разбивается на решение двух основных групп задач:

1) своевременное и полное удовлетворение информационных потребностей, возникающих в процессе управленческой,

инженерно-технической, маркетинговой и иной деятельности,

т.е. обеспечение специалистов организаций, предприятий и

фирм секретной или конфиденциальной информацией;

2) ограждение засекреченной информации от несанкционированного доступа к ней соперника, других субъектов в злонамеренных целях.

При решении первой группы задач учитывается, что специалисты могут использовать как открытую, так и засекреченную информацию. Снабжение специалистов открытой информацией ничем не ограничивается, кроме её фактического наличия. При снабжении же специалиста засекреченной информацией действуют ограничения: наличие соответствующего допуска

(к какой степени секретности информации он допущен) и разрешения на доступ к конкретной информации. В решении проблемы доступа специалиста к соответствующей засекреченной

информации всегда существуют противоречия: необходимо, с

одной стороны, максимально ограничить его доступ к засекреченной информации и тем самым уменьшить вероятность утечки этой информации, а с другой - наиболее полно удовлетворить его потребности в информации, в том числе и засекреченной, для обоснованного решения им служебных задач.

Вторая группа задач включает в себя такие условия, как:

- защита информационного суверенитета страны и расширение возможностей государства по укреплению своего могущества за счёт формирования и управления развитием своего

информационного потенциала;

- обеспечение безопасности защищаемой информации:

предотвращение хищения, утраты, несанкционированного уничтожения, модификации, блокирования информации и т.п., вмешательства в информацию и информационные системы;

- сохранение секретности информации в соответствии с

установленными правилами её защиты, в том числе предупреждение её утечки и несанкционированного доступа к её носителям;

- сохранение полноты, достоверности, целостности информации и её массивов и программ обработки;

- недопущение безнаказанного растаскивания и незаконного использования интеллектуальной собственности, принадлежащей государству.

Вопросы защиты государственной тайны приобрели особую значимость в последние годы, в период глубоких социально-экономических преобразований в РФ, когда, с одной стороны, появились новые угрозы безопасности государства, а, с другой стороны, сложившиеся режимы защиты государственной

тайны перестают срабатывать должным образом.

В ст. 2 Закона РФ «О государственной тайне» дано определение системы защиты государственной тайны.

Система защиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений,

составляющих государственную тайну, и их носителей,

а также мероприятий, проводимых в этих целях._____

Система защиты сведений, отнесенных к государственной

тайне, и их носителей складывается из:

- органов защиты государственной тайны;

- средств и методов защиты государственной тайны;

- проводимых мероприятий.

Защита сведений, составляющих государственную

тайну, и их носителей - деятельность органов защиты

этой тайны, направленная на обеспечение безопасности информации, отнесенной к государственной тайне,

предотвращение её утечки и её максимально эффективное использование.

Главным субъектом, осуществляющим защиту сведений,

составляющих государственную тайну, является государство в

лице его высших органов власти и управления, которое располагает всей полнотой властных полномочий по решению задач

защиты государственной тайны. В ст. 4 Закона РФ «О государственной тайне» определены полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защите. Распоряжением Президента РФ от 11 февраля 1994 г. № 73-рп утвержден перечень

должностных лиц органов государственной власти, наделяемых

полномочиями по отнесению сведений к государственной тайне.

Высшие органы государственной власти и управления создают нормативно-правовую базу, регламентирующую деятельность по защите сведений, отнесенных к государственной тайне.

Координация деятельности по разработке и выполнению государственных программ, по подготовке нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне, возложена на Межведомственную комиссию. Каждый орган и должностное лицо наделяются полномочиями по проведению организационно-правовых

мероприятий по защите государственной тайны (Закон РФ «О

государственной тайне», ст. 20).

В систему защиты государственной тайны включаются

кроме мер, осуществляемых непосредственно в местах сосредоточения и обращения сведений, составляющих эту тайну, также

проводимые государством мероприятия и устанавливаемые административно-правовые режимы:

- борьба со шпионажем и разглашением государственной тайны;
- охрана государственных тайн в печати;
- пограничный режим;
- режим въезда и передвижения иностранцев;
- режим выезда специалистов в служебные командировки

за границу.

Они в качестве составных элементов включаются в систему защиты государственной тайны и в большинстве своём играют роль препятствия, преграды в возможных каналах утечки

секретной информации.

Рассматривая проблемы деятельности по защите государственной тайны, можно назвать ряд факторов, которые предопределяют её формирование и состояние. Организация деятельности по защите государственных секретов в стране зависит от

военно-политической обстановки в мире и стране. Обострение

международной обстановки обычно приводит к усилению деятельности спецслужб противоборствующих сторон и соответственно к ужесточению принимаемых мер по защите своих секретов.

Уровень защиты секретной информации в определенной

степени должен соответствовать важности этой информации для

собственника и интенсивности действий потенциального противника по добыванию секретов о нашем государстве. Защита

секретов должна носить превентивный характер: меры защиты

секретной информации должны предупреждать возможность

несанкционированного доступа к засекреченной информации и

возможные вредные последствия, которые могут наступить в

случае утечки секретной информации.

Организация защиты государственной тайны находится в зависимости от принятой системы и критериев засекречивания информации: чем больше засекречивается информации, тем больше требуется сотрудников для её обработки, хранения и выдачи, тем выше стоимость её защиты; чем выше степень секретности информации, тем выше уровень её защиты, и т.д. После засекречивания информация начинает жить своей собственной жизнью: практически уже не имеет значения, произведено засекречивание сведений, действительно составляющих государственную тайну, или информация засекречена «на всякий случай», чтобы что-то скрыть и т.п. Секретная информация сама начинает «диктовать» условия своей защиты режимным службам и другим исполнителям.

Расширение круга засекречиваемых сведений и значительное увеличение в связи с этим количества секретной информации затрудняет её защиту, а увеличение числа лиц, допущенных к этой информации, усиливает вероятность её утечки. А это начинает противоречить одному из основных принципов защиты секретной информации - максимальному ограничению числа лиц, допускаемых к секретам.

Система защиты информации включает в себя совокупность элементов, её образующих, и их свойства. Внутренние связи системы и их свойства составляют архитектуру системы, её структуру и внутреннюю организацию. Одновременно элементы системы имеют внешние связи, которые целенаправленно воздействуют на внешнюю среду и решают поставленные перед системой задачи, это - функциональная часть системы. Вполне естественно, что обе части системы - структурная и функциональная - не отделены друг от друга: это как бы две стороны одних и тех же элементов, составляющих систему защиты информации.

Структурная часть системы защиты информации составляет её внутреннюю организацию, которая позволяет системе нормально функционировать, создает условия для обеспечения безопасности засекреченной информации, её обращения только по каналам, контролируемым данной системой.

Структурная часть системы защиты информации включает:

1) систему законов и других нормативных актов, устанавливающих:

- порядок и правила защиты информации, а также ответственность за покушение на защищаемую информацию или на установленный порядок её защиты;
- защиту прав граждан, связанных по службе со сведениями, отнесенными к охраняемой тайне;
- права и обязанности государственных органов, предприятий и должностных лиц в области защиты информации;

2) систему засекречивания информации, в которую входят:

- законодательное определение категории сведений, которые могут быть отнесены к государственной тайне;
- законодательное и иное правовое определение категорий сведений, которые не могут быть отнесены к государственной тайне;
- наделение полномочиями органов государственной власти и должностных лиц в области отнесения сведений к охраняемой законом тайне;
- составление перечней сведений, отнесенных к государственной тайне;

3) систему режимных служб и служб безопасности с их собственной структурой, штатным расписанием, обеспечивающими функционирование всей системы защиты информации.

Структурная часть системы защиты информации является устойчивой частью данной системы, её консервативной частью.

Как видно из перечисления основных элементов структурной
части системы, её элементы могут изменяться только «скачкообразно», они не могут приспосабливаться быстро и непрерывно в зависимости от изменения внешней среды, а также изменения обстановки, поскольку внешняя среда может оказывать
влияние на структурную часть системы защиты информации
лишь через её функциональную часть, т.е. опосредованно.

Функциональная часть системы защиты информации решает задачи обеспечения засекреченной информацией деятельности вышестоящей системы, в которую данная система защиты
информации «встроена». В эту деятельность вовлекается широкий
круг работников объекта: сотрудники службы безопасности,
связанные с обработкой, хранением, выдачей и учётом засекреченной информации; руководители объекта и структурных подразделений; исполнители, т.е. все работники объекта, которые
являются потребителями защищаемой информации. Способы зашиты государственной тайны

Основными организационными и техническими способами, используемыми в защите государственной тайны, являются:

скрытие, ранжирование, дробление, учёт, дезинформация, морально-нравственные меры, кодирование и шифрование.

Скрытие как метод защиты информации является в основе своей реализацией на практике одного из основных организационных принципов защиты информации - максимального ограничения числа лиц, допускаемых к секретам. Скрытие - один
из наиболее общих и широко применяемых методов защиты информации. Реализация этого метода достигается обычно путём:

- засекречивания информации, т.е. отнесения её к секретной или конфиденциальной информации различной степени
секретности и ограничения в связи с этим доступа к этой информации в зависимости от её важности для собственника, что
проявляется в проставляемом на носителе этой информации
грифе секретности;
- устранения или ослабления технических демаскирующих
признаков объектов защиты и технических каналов утечки сведений о них.

Ранжирование как метод защиты информации включает,
во-первых, деление засекречиваемой информации по степени
секретности и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций. Разграничение доступа к информации может
осуществляться по тематическому признаку или по признаку
секретности информации и определяется матрицей доступа.

Ранжирование как метод защиты информации является частным
случаем метода скрытия: пользователь не допускается к информации, которая ему не нужна для выполнения его служебных
функций, и тем самым эта информация скрывается от него и
всех остальных (посторонних) лиц.

Дезинформация - метод защиты информации, заключающийся в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий,
действительного состояния какой-то области государственной
деятельности. Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по внешнему
виду или проявлениям похожих на интересующие соперника
объекты, и др.

Дробление (расчленение) информации на части с таким

условием, что знание какой-то одной части информации (например, знание одной операции технологии производства какого-то продукта) не позволяет восстановить всю картину, всю

технологию в целом. Этот способ применяется достаточно широко при производстве средств вооружения и военной техники,

а также при производстве товаров народного потребления.

М орально-нравственные способы защиты информации

можно отнести к группе тех методов, которые, исходя из расхожего выражения, что «тайну хранят не замки, а люди», играют

очень важную роль в защите информации. Именно человек, сотрудник предприятия или учреждения, допущенный к секретам

и накапливающий в своей памяти колоссальные объёмы информации, в том числе секретной, нередко становится источником

утечки этой информации или по его вине соперник получает

возможность несанкционированного доступа к носителям защищаемой информации.

Морально-нравственные методы защиты информации

предполагают прежде всего воспитание сотрудника, допущенного к секретам, т.е. проведение специальной работы, направленной на формирование у него системы определенных качеств,

взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично), и обучение

сотрудника, осведомленного в сведениях, составляющих охраняемую тайну, правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Учёт также является одним из важнейших методов защиты

информации, обеспечивающим возможность получения в любое

время данных о любом носителе защищаемой информации, о

количестве и местонахождении всех носителей засекреченной

информации, а также данные обо всех пользователях этой информации. Без учёта решать проблемы было бы невозможно,

особенно когда количество носителей превысит какой-то минимальный объём.

Принципы учёта засекреченной информации:

1) обязательность регистрации всех носителей защищаемой информации;

2) однократность регистрации конкретного носителя такой

информации;

3) указание в учётах адреса, где находится в данное время

данный носитель засекреченной информации:

4) единоличная ответственность за сохранность каждого

носителя защищаемой информации и отражение в учётах пользователя данной информации в настоящее время, а также всех

предыдущих пользователей данной информации.

Кодирование - метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов

открытого текста в условный при передаче информации по каналам связи, направлении письменного сообщения, когда есть

угроза, что оно может попасть в руки соперника, а также при

обработке и хранении информации в средствах вычислительной

техники.

Для кодирования используются обычно совокупность знаков (символов, цифр и др.) и система определенных правил, при

помощи которых информация может быть преобразована (закодирована) таким образом, что прочесть её можно будет только

если потребитель располагает соответствующим ключом (кодом) для её раскодирования. Кодирование информации может

производиться с использованием технических средств или
вручную.

Ш ифрование - метод защиты информации, используемый
чаще при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником.

Шифрование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если
перехвативший не имеет сведений (ключа) для раскрытия шифра.

Шифрование может быть предварительным (шифруется
текст документа) и линейным (шифруется разговор). Для шифрования информации может использоваться специальная аппаратура.

Знание возможностей приведенных методов позволяет активно и комплексно применять их при рассмотрении и использовании правовых, организационных и инженерно-технических
мер защиты секретной информации.

Режим секретности

При рассмотрении проблем защиты информации часто затрагивается вопрос о режиме секретности или конфиденциальности (в дальнейшем - режим секретности). Понятие «режим
секретности» тесно связано с понятием «защита информации»,
переплетается с ним, а иногда и отождествляется.

Режим секретности является частью системы защиты засекреченной информации, а точнее, это реализация системы защиты информации для конкретного объекта или одного из его
сгруктурных подразделений или конкретной работы.

Основное назначение режима секретности - обеспечить
соответствующий уровень защиты информации, т.к. чем выше
степень её секретности, тем более высокий уровень её защиты
устанавливается, соответственно изменяется и режим секретности. Режим секретности - это не регламентация правовых норм
и правил защиты сведений, а реализация на конкретном объекте
действующих норм и правил защиты сведений, составляющих
государственную тайну, установленных и регламентированных
соответствующими законодательными и подзаконными нормативными актами.

Режим секретности включает следующие группы мер:

- разрешительную систему, определяющую порядок доступа в служебных целях конкретных сотрудников к определенной защищаемой информации и в конкретные помещения, где
ведутся конфиденциальные или секретные работы;
- порядок и правила делопроизводства с секретными или
конфиденциальными документами и иными носителями защищаемой информации. Возможно разделение потоков документальной
информации по степени секретности сведений, содержащихся в
документах, а также разделение потоков информации, документов, содержащих государственную и коммерческую тайну;
- установление пропускного и внутри объектового режима,
соответствующего степени секретности информации, имеющейся
на объекте;
- воспитательно-профилактическую работу, уровень и содержание которой должны соответствовать уровню требуемой
защиты информации с целью предотвратить или значительно
уменьшить риск утечки засекреченной информации через сотрудников объекта, работающих с такой информацией.

В рамках установленного на объекте режима секретности
проводятся все остальные мероприятия по защите сведений, составляющих государственную тайну.

6. Правовое направление обеспечения информационной безопаности

Как известно, право — это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и на селения (отдельной личности).

Правовая защита информации как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном уровне правовая защита регулируется государственными и ведомственными актами (рис. 11). В нашей стране такими правилами (актами, нормами) являются Конституция, законы Российской Федерации, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Что касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, издаваемыми ведомствами, организациями и предприятиями, действующими в рамках определенных структур (рис. 12). Современные условия требуют и определяют необходимость комплексного подхода к формированию законодательства по защите информации, его состава и содержания, соотнесения его со всей системой законов и правовых актов Российской Федерации. Требования информационной безопасности должны органически включаться во все уровни законодательства, в том числе и в конституционное законодательство, основные общие законы, законы по организации государственной системы управления, специальные законы, ведомственные правовые акты и другие. В литературе приводится такая структура правовых актов, ориентированных на правовую защиту информации. Первый блок — конституционное законодатель ство. Нормы, касающиеся вопросов информатизации и защиты информации, входят в него как составные элементы. Второй блок — общие законы, кодексы (о собственности, о недрах, о земле, о правах граждан, о граждан стве, о налогах, об антимонопольной деятельности), ко торые включают нормы по вопросам информатизации и информационной безопасности. Третий блок — законы об организации управле ния, касающиеся отдельных структур хозяйства, эко номики, системы государственных органов и определяющие их статус. Они включают отдельные нормыпо вопросам защиты информации. Наряду с общими вопросами информационного обеспечения и защиты информации конкретного органа эти нормы должны устанавливать его обязанности по формированию, актуализации и безопасности информации, представляющей общегосударственный интерес. Четвертый блок — специальные

законы, полнос тью относящиеся к конкретным сферам отношений, отраслям хозяйства, процессам. В их число входит и Закон РФ «Об информации, информатизации и защи те информации». Именно состав и содержание этого блока законов и создает специальное законодательство как основу правового обеспечения информационной безопасности. Пятый блок — законодательство субъектов Российской Федерации, касающееся защиты информации. Шестой блок — подзаконные нормативные акты по защите информации. Седьмой блок — это правоохранительное законодательство России, содержащее нормы об ответствен ности за правонарушения в сфере информатизации. Специальное законодательство в области безопас ности информационной деятельности может быть представлено совокупностью законов. В их составе особое место принадлежит базовому Закону «Об информации, информатизации и защите информации», который закладывает основы правового определения всех важнейших компонентов информационной дея тельности: ■ информации и информационных систем; ■ субъектов — участников информационных процессов; ■ правоотношений производителей — потребителей информационной продукции; ■ владельцев (обладателей, ис точников) информации — обработчиков и потребителей на основе отношений собственности при обеспечении гаран тий интересов граждан и государства. Этот закон определяет основы защиты информации в системах обработки и при ее использовании с учетом категорий доступа к открытой информации и к информации с ограниченным доступом. Этот закон содержит, кроме того, общие нормы по организации и ведению информационных систем, включая банки данных государственного назначения, порядка государ ственной регистрации, лицензирования, сертификации, экспертизы, а также общие принципы защиты и гарантий прав участников информационного процесса. В дополнение к базовому закону в мае 1992 г. Были приняты Законы «О правовой охране программ для электронновычислительных машин и баз данных» и «О правовой охране топологии интегральных микросхем». Оба закона устанавливают охрану соответствующих объектов с помощью норм авторского права, включая в перечень объектов авторского права наря ду с традиционными базами данных топологии интег ральных микросхем и программы для ЭВМ. Вопросы правового режима информации с ограниченным доступом реализуются в двух самостоятель ных законах о государственной и коммерческой (проект) тайнах. Кроме того, этот аспект раскрывается и в Гражданском кодексе РФ статьей 139 «Служебная и коммерческая тайна». 1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну,

определяются законом и иными правовыми актами. 2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим кодексом и другими зако нами. Вторая часть статьи 139 определяет правовые основы ответственности за несанкционированное получение информации или причинение ущерба. Звучит это так: «Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору». Указ Президента РФ от 6 марта 1997 г. № 188 оп ределяет понятие и содержание конфиденциальной информацииТаким образом, правовая защита информации обеспечивается нормативно-законодательными актами, представляющими собой по уровню иерархическую систему от Конституции РФ до функциональныхобязанностей и контракта отдельного конкретного исполнителя, определяющих перечень сведений, подлежащих охране, и меры ответственности за их разглашение. Одним из новых для нас направлений правовой защиты является страховое обеспечение. Оно предназначено для защиты собственника информации и средств ее обработки как от традиционных угроз (кражи, стихийные бедствия), так и от угроз, возникающих в ходе работы с информацией. К ним относятся: разглашение, утечка и несанкционированный доступ к конфиденциальной информации. Целью страхования является обеспечение страхо вой защиты физических и юридических лиц от стра ховых рисков в виде полного или частичного возмещения ущерба и потерь, причиненных стихийными бедствиями, чрезвычайными происшествиями в различных областях деятельности, противоправными действиями со стороны конкурентов и злоумышленников путем выплат денежной компенсации или оказания сервисных услуг (ремонт, восстановление) при наступ - лении страхового события. В основе российского страхового законодательства лежит Закон РФ «О страховании». Он призван гаран тировать защиту интересов страхователей, определять единые положения по организации страхования и принципы государственного регулирования страховой деятельности. Закон «О страховании» дает следующее понятие страхования: «Страхование представляет собой отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страхо вых взносов». Действия по защите информации от утечки по техническим каналам регламентируются следующими правовыми документами: 1. ГОСТ 29339-92 «Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ». (ПЭМИН — побочные электромагнитные излучения и наводки.). 2. ГОСТ Р 50752 «Информационная технология. Защита информации от

утечки за счет ПЭМИН при ее обработке средствами вычислительной техники. Методы испытаний». 3. Нормы эффективности и защиты АСУ и ЭВМ от утечки информации за счет ПЭМИН. 4. Специальные требования и рекомендации по за щите объектов ЭВТII и III категории от утечки информации за счет ПЭМИН. Действия по защите информации от несанкциони рованного доступа (НСД) регламентируют Постановление Правительства РФ от 15.09.93 № 912-51 «Положение о государственной системе защиты информации от иностранной технической разведки и от утечки по техническим каналам», а также Указы Президента РФ «О создании государственной технической комиссии при Президенте РФ» (от 05.01.92 № 9); «О защите информационнотелекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам связи» (от 08.05.93 № 644); «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (от 03.04.95 № 334); «Положение о государственной системе защиты информации в Российской Федерации». Правовыми документами являются и государ ственные стандарты на информационную деятель ность с учетом обеспечения ее безопасности, в частности ГОСТ Р 50739-95 «СВТ. Защита от НСД к информации»; ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»; ГОСТ Р.34.10-94 «Процедуры выработки и проверки электронной подписи на базе асимметрического криптографического алгоритма»; ГОСТ Р.34.11-94 «Функция хэширования»; ГОСТ Р.В.50170-92 «Противодействие ИТР. Термины и определения». Опираясь на государственные правовые акты и учитывая ведомственные интересы на уровне конкретного предприятия (фирмы, организации), разрабатываются собственные нормативноправовые документы, ориентированные на обеспечение информационной безопасности. К таким документам относятся: ■ Положение о сохранении конфиденциальной информации; ■ Перечень сведений, составляющих конфиденци альную информацию; ■ Инструкция о порядке допуска сотрудников к све дениям, составляющим конфиденциальную информацию; ■ Положение о специальном делопроизводстве и документообороте; ■ Перечень сведений, разрешенных к опубликова нию в открытой печати; ■ Положение о работе с иностранными фирмами и их представителями; ■ Обязательство сотрудника о сохранении конфиденциальной информации; ■ Памятка сотруднику о сохранении коммерческой тайны. Указанные нормативные акты направлены на пре - дупреждение случаев неправомерного оглашения (разглашения) секретов на правовой основе, и в случае их нарушения должны приниматься соответствующие меры воздействия. В зависимости от характера информации, ее доступности для заинтересованных потребителей, а также

экономической целесообразности конкретных защитных мер могут быть избраны следующие формы защиты информации: ■ патентование; ■ авторское право; ■ признание сведений конфиденциальными; ■ товарные знаки; ■ применение норм обязательственного права.

Существуют определенные различия между авторским правом и коммерческой тайной. Авторское правозащищает только форму выражения идеи. Коммерческая тайна относится непосредственно к содержа нию. Авторское право защищает от копирования не зависимо от конфиденциальных отношений с владельцем. К авторскому праву прибегают при широкой публикации своей информации, в то время как коммерческую тайну держат в секрете. Очевидно, что по сравнению с патентом и авторским правом, коммерческая и производственная тайны являются наиболее удобными, надежными и гибкими формами защиты информации. Помимо вышеизложенных форм правовой защи ты и права принадлежности информации находит ши рокое распространение официальная передача права на пользование ею в виде лицензии. Лицензия — это разрешение, выдаваемое государством на проведение некоторых видов хозяйственной деятельности, вклю чая внешнеторговые операции (ввоз и вывоз) и предоставление права использовать защищенные патентами изобретения, технологии, методики. Лицензионные разрешения предоставляются на определенное время и на определенные виды товаров. На все эти формы защиты интеллектуальной собственности имеются соответствующие законы РФ — закон о патентах, закон об авторском праве, проект закона о коммерческой тайне, закон о товарных знаках и другие. Создавая систему информационной безопасности, необходимо четко понимать, что без правового обеспечения защиты информации любые последующие претензии с вашей стороны к недобросовестному сотруднику, клиенту, конкуренту и должностному лицу окажутся просто беспочвенными. Если перечень сведений конфиденциального ха рактера не доведен своевременно до каждого сотрудника (естественно, если он допущен по должностным обязанностям) в письменном виде, то сотрудник, укравший важную информацию в нарушение установ - ленного порядка работы с ней, скорее всего разведет руками: мол, откуда мне это знать! В этом случае никакие инстанции, вплоть до судебных, не смогут Вам помочь. Правовые нормы обеспечения безопасности и защиты информации на конкретном предприятии (фирме, организации) отражаются в совокупности учредительных, организационных и функциональных документов. Требования обеспечения безопасности и защиты информации отражаются в Уставе (учредительном договоре) в виде следующих положений: ♣ предприятие имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, требовать от своих сотрудников обеспечения их сохранности и защиты от внутренних и внешних угроз; ♣ предприятие обязано обеспечить сохранность конфиденциальной информации.

Такие требования дают право администрации предприятия: ♣ создавать организационные структуры по защите конфиденциальной информации; ♣ издавать нормативные и распорядительные доку менты, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты; ♣ включать требования по защите информации в договоры по всем видам хозяйственной деятельности; ♣ требовать защиты интересов предприятия со стороны государственных и судебных инстанций; ♣ распоряжаться информацией, являющейся собственностью предприятия, в целях извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств производства; ♣ разработать «Перечень сведений конфиденциаль ной информации». Требования правовой обеспеченности защиты информации предусматриваются в коллективном договоре. Коллективный договор должен содержать следующие требования: Раздел «Предмет договора» Администрация предприятия (в том числе и администрация самостоятельных подразделений) обязуется обеспечить разработку и осуществление мероприятий по определению и защите конфиденциальной информации. Трудовой коллектив принимает на себя обязатель ства по соблюдению установленных на предприятии требований по защите конфиденциальной информации. Администрация обязана учесть требования защи ты конфиденциальной информации в правилах внутреннего распорядка. Раздел «Кадры. Обеспечение дисциплины труда» Администрация обязуется: нарушителей требований по защите коммерческой тайны привлекать к административной и уголовной ответственности в соответствии с действующим законодательством. Правила внутреннего трудового распорядка для рабочих и служащих предприятия целесообразно дополнить следующими требованиями. Раздел «Порядок приема и увольнения рабочих и служащих» ♣ При поступлении рабочего или служащего на работу или переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией предприятия, а также при увольне нии администрация обязана проинструктировать работника или служащего по правилам сохранения коммерческой тайны с оформлением письменного обязательства о ее неразглашении. ♣ Администрация предприятия вправе принимать решение об отстранении от работ лиц, которые нарушают установленные требования по защите конфиденциальной информации. Раздел «Основные обязанности рабочих и служащих» Рабочие и служащие обязаны соблюдать требования нормативных документов по защите конфиденци альной информации предприятия. Раздел «Основные обязанности администрации» Администрация предприятия, руководители подразделений обязаны: ♣ обеспечить строгое сохранение конфиденциаль ной информации, постоянно осуществлять организаторскую и воспитательно-профилактическую работу, направленную на защиту секретов предприятия; ♣ включить в должностные инструкции и положе ния

обязанности по сохранению конфиденциаль ной информации; ♣ неуклонно выполнять требования Устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других организационных и хозяйственных документов в части обеспечения экономической и информационной безопасности. Обязательства конкретного сотрудника, рабочего или служащего в части защиты информации обязательно должны быть оговорены в трудовом договоре (контракте). В соответствии с КЗоТ (гл. III) при заключении трудового договора трудящийся обязуется выполнять определенные требования, действующие на данном предприятии. Независимо от формы заключения договора (устного или письменного) подпись трудящегося на приказе о приеме на работу подтверждает его согласие с условиями договора (КЗоТ РФ ст. 18). Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действуют требования по защите информации, вытекающие из нормативно-правовых документов предприятия. При заключении трудового договора и оформлении прика за о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент включения данного лица в механизм обеспе - чения информационной безопасности. Использование договоров о неразглашении тай ны — вовсе не самостоятельная мера по ее защите. Не следует думать, что после подписания такого соглашения с новым сотрудником тайна будет сохранена. Это только предупреждение сотруднику, что в дело вступает система мероприятий по защите информации, и 'правовая основа к тому, чтобы пресечь его неверные или противоправные действия. Дальше задача — не допустить утраты коммерческих секретов. Реализация правовых норм и актов, ориентирован ных на защиту информации на организационном уровне, опирается на те или иные организационно-правовые формы, к числу которых относятся соблюдение конфиденциальности работ и действий, договоры (со глашения) и различные формы обязательного права. Конфиденциальность — это форма обращения со сведениями, составляющими коммерческую тайну, на основе организационных мероприятий, исключающих неправомерное овладение такими сведениями. Договоры — это соглашения сторон (двух и более лиц) об установлении, изменении или прекращении взаимных обязательств. Обязательство — гражданское правоотношение, в силу которого одна сторона (должник) обязана совер шить в пользу другой стороны определенные действия (рис. 13). Правовое регулирование необходимо для совершенствования механизма предупреждения противоправных действий по отношению к информационным ресурсам, для уточнения и закрепления задач и правомочий отдельных субъектов в сфере предупредительной деятельности, охраны прав и законных инте - ресов граждан и организаций. Анализ

законодательства, регулирующего деятель ность субъектов в сфере информационной безопасности, показывает наличие определенных недостатков. Существующие правовые нормы разбросаны по различным нормативным актам, издававшимся в разное время, в разных условиях и на разных уровнях. Действующее законодательство не систематизировано, что создает большие трудности в его использовании на практике. Правовые меры обеспечения безопасности и защиты информации являются основой порядка деятельности и поведения сотрудников предприятия и определяют меры их ответственности за нарушение установленных норм.

7. Организационное направление обеспечения информационной безопасности

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз. Организационная защита обеспечивает: ♣ организацию охраны, режима, работу с кадрами, с документами; ♣ использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности. Организационные мероприятия играют существен ную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадиво стью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационноправовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникно вения опасности конфиденциальной информации. К основным организационным мероприятиям можно отнести: ♣ организацию режима и охраны. Их цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.; ♣ организацию работы с сотрудниками, которая предусматривает подбор и расстановку персона ла, включая ознакомление с сотрудниками, их изу чение, обучение правилам работы с конфиденциальной

информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.; ♣ организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение; ♣ организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации; ♣ организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты; ♣ организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хра нения и уничтожения документов и технических носителей (рис. 14). В каждом конкретном случае организационные мероприятия носят специфическую для данной организации формуй содержание, направленные на обес печение безопасности информации в конкретных ус ловиях. Специфической областью организационных мер является организация защиты ПЭВМ, информационных систем и сетей. Организация защиты ПЭВМ, информационных систем и сетей определяет порядок и схему функционирования основных ее подсистем, использование устройств и ресурсов, взаимоотношения пользователей между собой в соответствии с нормативноправовыми требованиями и правилами. Защита информации на основе организационных мер играет большую роль в обеспечении надежности и эффективности, так как несанкционированный доступ и утечка информации чаще всего обусловлены злоумышленными действиями, небрежностью пользова телей или персонала. Эти факторы практически не возможно исключить или локализовать с помощью аппаратных и программных средств, криптографии и физических средств защиты. Поэтому совокупность организационных, организационно-правовых и организационно-технических мероприятий, применяемых совместно с техническими методами, имеют цель исключить, уменьшить или полностью устранить потери при действии различных нарушающих факторов. Организационные средства защиты ПЭВМ и информационных сетей применяются: ■ при проектировании, строительстве и оборудовании помещений, узлов сети и других объектов информационной системы, исключающих влияние стихийных бедствий, возможность недозволенно го проникновения в помещения и др.; ■ при подборе и подготовке персонала. В этом случае предусматриваются проверка принимаемых на работу, создание условий, при которых персонал был бы заинтересован в сохранности данных, обу чение правилам работы с закрытой информацией, ознакомление с мерами ответственности за нарушение правил защиты и др.; ■ при хранении и использовании документов и других носителей (маркировка, регистрация, определение правил выдачи и возвращения, ведение до кументации и др.); ■ при соблюдении надежного пропускного режима к

техническим средствам, к ПЭВМ и информационным системам при сменной работе (выделение ответственных за защиту информации в сменах, контроль за работой персонала, ведение (возможно и автоматизированное) журналов работы, уничтожение в установленном порядке закрытых производственных документов) ; ■ при внесении изменений в программное обеспечение (строгое санкционирование, рассмотрение и утверждение проектов изменений, проверка их на удовлетворение требованиям защиты, документальное оформление изменений и др.); ■ при подготовке и контроле работы пользователей. Одним из важнейших организационных мероприятий является создание специальных штатных служб защиты информации в закрытых информационных системах в виде администратора безопасности сети и администратора распределенных баз и банков данных, содержащих сведения конфиденциального характера. Очевидно, что организационные мероприятия должны четко планироваться, направляться и осуществляться какой-то организационной структурой, каким-то специально созданным для этих целей структурным подразделением, укомплектованным соответствующими специалистами по безопасности предпринимательской деятельности и защите информации. Зачастую таким структурным подразделением яв ляется служба безопасности предприятия (фирмы, организации), на которую возлагаются следующие общие функции: ♣ организация и обеспечение охраны персонала, материальных и финансовых ценностей и защиты конфиденциальной информации; ♣ обеспечение пропускного и внутриобъектового режима на территории, в зданиях и помещениях, контроль соблюдения требований режима сотрудниками, смежниками, партнерами и посетителями; ♣ руководство работами по правовому и организационному регулированию отношений по защите информации; ♣ участие в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты информации, а также положений о подразделениях, трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специали стов, рабочих и служащих; ♣ разработка и осуществление совместно с другими подразделениями мероприятий по обеспечению работы с документами, содержащими конфиденциальные сведения; при всех видах работ организация и контроль выполнения требований «Инструкции по защите конфиденциальной информации»; ♣ изучение всех сторон производственной, коммерческой, финансовой и другой деятельности для выявления и последующего противодействия лю бым попыткам нанесения ущерба, ведения учета и анализа нарушений режима безопасности, накопление и анализ данных о злоумышленных ус тремлениях конкурентной и других организаций, о дея тельности предприятия и его клиентов, партнеров, смежников; ♣ организация и проведение служебных расследований по фактам разглашения сведений, утрат документов, утечки конфиденциальной информации и

других нарушений безопасности предприятия; ♣ разработка, ведение, обновление и пополнение «Перечня сведений конфиденциального характе ра» и других нормативных актов, регламентирующих порядок обеспечения безопасности и защиты информации; ♣ обеспечение строгого выполнения требований нормативных документов по защите производственных секретов предприятия; ♣ осуществление руководства службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и другими структурами в части оговоренных в договорах условий по защите конфиденциальной информации; ♣ организация и регулярное проведение учета сотрудников предприятия и службы безопасности по всем направлениям защиты информации и обеспечения безопасности производственной деятельности; ♣ ведение учета и строгого контроля выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации и каналами проникновения к источникам охраняемых секретов; ♣ обеспечение проведения всех необходимых мероприятий по пресечению попыток нанесения морального и материального ущерба со стороны внутренних и внешних угроз; ♣ поддержание контактов с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне) и оказания взаимной помощи в кризисных ситуациях. Служба безопасности является самостоятельной организационной единицей предприятия, подчиняю щейся непосредственно руководителю предприятия. Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности. Организационно служба безопасности состоит из следующих структурных единиц: ♣ подразделения режима и охраны; ♣ специального подразделения обработки документов конфиденциального характера; ♣ инженерно-технических подразделений; ♣ информационно-аналитических подразделений. В таком составе служба безопасности способна обеспечить защиту конфиденциальной информации от любых угроз. К задачам службы безопасности предприятия относятся: ♣ определение круга лиц, которые в силу занимаемого служебного положения на предприятии прямо или косвенно имеют доступ к сведениям конфиденциального характера; ♣ определение участков сосредоточения конфиден циальных сведений; ♣ определение круга сторонних предприятий, свя занных с данным предприятием кооперативными связями, на которых в силу производственных отношений возможен выход из-под контроля сведений конфиденциального характера; ♣ выявление круга лиц, не допущенных к конфиденциальной информации, но проявляющих повы шенный интерес к таким сведениям; ♣ выявление круга предприятий, в том числе и иностранных, заинтересованных в овладении охраняе мыми сведениями с целью нанесения

экономического ущерба данному предприятию, устранения экономического конкурента либо его компрометации; ♣ разработка системы защиты документов, содержащих сведения конфиденциального характера; ♣ определение на предприятии участков, уязвимых в аварийном отношении, выход из строя которых может нанести материальный ущерб предприятию и сорвать поставки готовой продукции или комплектующих предприятиям, связанным с ним коо перацией; ♣ определение на предприятии технологического оборудования, выход (или вывод) которого из строя может привести к большим экономическим потерям; ♣ определение уязвимых мест в технологии производственного цикла, несанкционированное изменение в которой может привести к утрате качества выпускаемой продукции и нанести материальный или моральный ущерб предприятию (потеря конкурентоспособности); ♣ определение мест на предприятии, несанкциони рованное посещение которых может привести к изъятию (краже) готовой продукции или полуфабрикатов, заготовок и др. и организация их физической защиты и охраны; ♣ определение и обоснование мер правовой, организационной и инженерно-технической защиты предприятия, персонала, продукции и информации; ♣ разработка необходимых мероприятий, направлен ных на совершенствование системы экономической, социальной и информационной безопасности предприятия; ♣ внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической и информационной безопасности; ♣ организация обучения сотрудников службы безопасности в соответствии с их функциональными обязанностями; ♣ изучение, анализ и оценка состояния обеспечения экономической и информационной безопасности предприятия и разработка предложений и рекомендаций для их совершенствования; ♣ разработка технико-экономических обоснований, направленных на приобретение технических средств, получение консультации у специалис тов, разработку необходимой документации в целях совершенствования системы мер по обеспечению экономической и информационной безопасности. Организационные меры являются решающим звеном формирования и реализации комплексной защиты информации и созда ния системы безопасности предприятия.

Инженерно-техническая защита (ИТЗ) по опреде лению — это совокупность специальных органов, технических средств и мероприятий по их использова нию в интересах защиты конфиденциальной информации. Многообразие целей, задач, объектов защиты и проводимых мероприятий предполагает рассмотрение некоторой системы классификации средств по виду, ориентации и другим характеристикам. Например, средства инженерно-технической защиты можно рассматривать по объектам их воздействия. В этом плане они могут применяться для защиты людей,

материальных средств, финансов, информации. Примерная классификационная структура инженернотехнической защиты приведена на рис.15. Многообразие классификационных характеристик позволяет рассматривать инженерно-технические средства по объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны службы безопасности. По функциональному назначению средства инженернотехнической защиты делятся на следующие группы: ♣ физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышлен- ников на объекты защиты и к материальным носителям конфиденциальной информации (рис. 16) и осуществляющие защиту персонала, материаль ных средств, финансов и информации от противоправных воздействий; ■ аппаратные средства. Сюда входят приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность. Основная задача аппаратных средств — обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности; ■ программные средства, охватывающие специаль ные программы, программные комплексы и системы защиты информации в информационных систе мах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и пере дачи) данных; ■ криптографические средства— это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования. Аппаратные средства и методы защиты распространены достаточно широко. Однако из-за того, что они не обладают достаточной гибкостью, часто теряют свои защитные свойства при раскрытии их принципов действия и в дальнейшем не могут быть используемы. Программные средства и методы защиты надежны и период их гарантированного использования без перепрограммирования значительно больше, чем аппаратных. Криптографические методы занимают важное место и выступают надежным средством обеспечения защиты информации на длительные периоды. Очевидно что такое деление средств защиты информации достаточно условно, так как на практике очень часто они: и взаимодействуют и реализуются в комплексе в виде программно - аппаратных модулей с широким использованием алгоритмов закрытия информации.

2.3.2. Физические средства защиты [^] Физические средства защиты — это разнообразные устройства, приспособления, конструкции, аппа раты, изделия,

предназначенные для создания препятствий на пути движения злоумышленников. К физическим средствам относятся механические, электромеханические электронные, электронно-оптические, радиои радиотехнические и другие устройства для воспрещение несанкционированного доступа (вхо да выхода) проноса (выноса) средств и материалов и других возможна видов преступных действий (рис. 17). Эти средств применяются для решения следую щих задач: 1. охрана территории предприятия и наблюдение за ней; 2. охрана зданий» внутренних помещений и контроль за ними; 3. охрана оборудования, продукции, финансов и информации; 4. осуществление контролируемого доступа в здания и помещения. Все физические средства защиты объектов можно разделить на три категории: средства предупрежде ния средства обнаружения и системы ликвидации угроз. Охранив сигнализация и охранное телевидение например, относятся к средствам обнаружения угроз; заборы вокруг объектов — это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов и т.д.) Средства пожаротушения относятся к системам ликвидации угроз. В общем плане по физической природе и функци ональному назначению все средства этой категории можно разделить на следующие группы: ♣ охранные и охранно-пожарные системы; ♣ охранное телевидение; ♣ охранное освещение; ♣ средства физической защиты.

Охранные системы

Охранные системы и средства охранной сигнали зации предназначены для обнаружения различных видов угроз: попыток проникновения на объект защиты, в охраняемые зоны и помещения, попыток проноса (выноса) оружия, средств промышленного шпионажа, краж материальных и финансовых ценностей и других действий; оповещения сотрудников охраны или персонала объекта о появлении угроз и необходимости усиления контроля доступа на объект, территорию, в здания и помещения. Важнейшими элементами охранных систем являются датчики, обнаруживающие появление угрозы. Характеристики и принципы работы датчиков определяют основные параметры и практические возможности охранных систем. Уже разработано и широко используется значительное количество самых разнообразных датчиков как по принципам обнаружения различных физических полей, так и по тактическому использованию. Эффективность работы системы охраны и охран ной сигнализации в основном определяется параметрами и принципом работы датчиков. На сегодня известны датчики следующих типов: механические выключатели, проволока с выключателем, магнитный выключатель, ртутный выключатель, коврики давле ния, металлическая фольга, проволочная

сетка, шифроволновый датчик, ультразвуковой датчик, инфракрасный датчик, фотоэлектрический датчик, акустический датчик, вибрационный датчик, индуктивный датчик, емкостный датчик и другие. Каждый тип датчика реализует определенный вид защиты: точечная защита, защита по линии, защита по площади или защита по объему. Механические датчики ориентированы на защиту линии, коврики давления — на точечное обнаружение, а инфракрасные находят широкое применение по площади и по объему. Датчики посредством тех или иных каналов связи соединены с контрольно-приемным устройством пункта (или поста) охраны и средствами тревожного опо вещения. Каналами связи в системах охранной сигнализа ции могут быть специально проложенные проводные или кабельные линии, телефонные линии объекта, линии связи трансляции, системы освещения или радиоканалы. Выбор каналов определяется возможностями объекта. Важным объектом охранной системы являются средства тревожного оповещения: звонки, лампочки, сирены, подающие постоянные или прерываемые сигналы о появлении угрозы. По тактическому назначению охранные системы подразделяются на системы охраны: ♣ периметров объектов; ♣ помещений и проходов в служебных и складских зданиях; ♣ сейфов, оборудования, основных и вспомогатель ных технических средств; ♣ автотранспорта; ♣ персонала, в том числе и личного состава охраны, и другие. К средствам физической защиты относятся: ♣ естественные и искусственные барьеры; ♣ особые конструкции периметров, проходов, окон ных и дверных переплетов, помещений, сейфов, хранилищ; ♣ зоны безопасности. Естественные и искусственные барьеры служат для противодействия незаконному проникновению на территорию объекта. Однако основная защитная на грузка ложится все-таки на искусственные барьеры — такие, как заборы и другие виды ограждений. Практика показывает, что ограждения сложной конфигурации способны задержать злоумышленника на достаточно большое время. На сегодня насчитывается значительный арсенал таких средств: от простых сетчатых до сложных комбинированных ограждений, оказывающих определенное отпугивающее воздей - ствие на нарушителя. Особые конструкции периметров, проходов, окон ных переплетов, помещений, сейфов, хранилищ являются обязательными с точки зрения безопасности для любых организаций и предприятий. Эти конструкции должны противостоять любым способам физического воздействия со стороны криминальных элементов: механическим деформациям, разрушению сверлением, термическому и механическому резанию, взрыву; несанкционированному доступу путем подделки ключей, угадывания кода и т. д. Одним из главных технических средств защиты проходов, помещений, сейфов и хранилищ являются замки. Они бывают простыми (с ключами), кодовыми (в том числе и с временной задержкой на открывание) и с программными устройствами, открывающие двери и сейфы только в определенные часы. Зоны безопасности. Важнейшим средством физи ческой

защиты является планировка объекта, его зда ний и помещений по зонам безопасности, которые учитывают степень важности различных частей объекта с точки зрения нанесения ущерба от различного вида угроз. Оптимальное расположение зон безопасности и размещение в них эффективных технических средств обнаружения, отражения и ликвидации последствий противоправных действий составляет основу концеп ции инженерно-технической защиты объекта. Зоны безопасности должны располагаться на объекте последовательно, от забора вокруг территории объекта до хранилищ ценностей, создавая цепь чередующихся друг за другом препятствий (рубежей), ко торые придется преодолевать злоумышленнику. Чем сложнее и надежнее препятствие на его пути, тем больше времени потребуется на преодоление каждой зоны и тем больше вероятность того, что расположен ные в каждой зоне средства обнаружения (охранные посты, охранная сигнализация и охранное телевиде ние) выявят наличие нарушителя и подадут сигнал тревоги. Основу планировки и оборудования зон безопасности объекта составляет принцип равнопрочности границ зон безопасности. Суммарная прочность зон безопасности будет оцениваться наименьшей из них.

Охранное телевидение

Одним из распространенных средств охраны является охранное телевидение. Привлекательной особенностью охранного телевидения является возможность не только отметить нарушение режима охраны объекта, но и контролировать обстановку вокруг него в динамике ее развития, определять опасность дей ствий, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения как с целью анализа, так и для привлечения к ответственности нарушителя. Источниками изображения (датчиками) в системах охранного телевидения являются видеокамеры. Через объектив изображение злоумышленника попадает на светочувствительный элемент камеры, в котором оно преобразуется в электрический сигнал, поступающий затем по специальному коаксиальному кабелю на монитор и при необходимости — на видеомагнитофон. Видеокамера является наиболее важным элемен том системы охранного телевидения, так как от ее характеристик зависит эффективность и результативность всей системы контроля и наблюдения. В настоящее время разработаны и выпускаются самые разнообразные модели, различающиеся как по габаритам, так и по возможностям и по конструктивному исполнению. Вторым по значимости элементом системы охран ного телевидения является монитор. Он должен быть согласован по параметрам с видеокамерой. Часто используется один монитор с несколькими камерами, подсоединяемыми к нему поочередно средствами автоматического переключения по определенному регламенту. В некоторых системах телевизионного наблюде ния предусматривается возможность автоматическо го подключения камеры, в зоне

обзора которой произошло нарушение. Используется и более сложное оборудование, включающее средства автоматизации, __ устройства одновременного вывода нескольких изображений, детекторы движения для подачи сигнала тревоги при выявлении каких-либо изменений в изображении.

Охранное освещение

Обязательной составной частью системы защиты любого объекта является охранное освещение. Разли чают два вида охранного освещения — дежурное и тревожное. Дежурное освещение предназначается для постоянного использования в нерабочие часы, в вечернее и ночное время как на территории объекта, так и внутри здания. Тревожное освещение включается при поступле нии сигнала тревоги от средства охранной сигнализа ции. Кроме того, по сигналу тревоги в дополнение к освещению могут включаться и звуковые приборы (звонки, сирены и пр.). Сигнализация и дежурное освещение должны иметь резервное электропитание на случай аварии или выключения электросети.

Ограждения и физическая изоляция

В последние годы большое внимание уделяется созданию систем физической защиты, совмещенных с системами сигнализации. Так, известна электронная система сигнализации для использования с проволочным заграждением. Система состоит из электронных датчиков и микропроцессора, управляющего блаком обработки данных. Заграждение длиной до 100 м может устанавливаться на открытой местности или размещаться на стенах, чердаках и имеющихся оградах. Устойчивые к воздействию окружающей среды датчики монтируются на стойках, кронштейнах. Прово лочное заграждение состоит из 32 горизонтально на тянутых стальных нитей, в средней части каждой из которых крепится электромеханический датчик, преобразующий изменение натяжения нитей в электри ческий сигнал. Превышение пороговой величины напряжения, программируемое по амплитуде для каждого датчика отдельно, вызывает сигнал тревоги. Связь системы с центральным пунктом управления и контроля осуществляется с помощью мультиплексора. Микропроцессор автоматически через определенные интервалы времени проверяет работу компонентов аппаратуры и программных средств и — в случае установления отклонений — подает соответствующий сигнал. Подобные и ряд других аналогичных систем физической защиты могут использоваться для защиты объектов по периметру в целях обнаружения вторжения на территорию объекта. Используются системы из сетки двух волоконно-оптических кабелей, по которым передаются кодированные сигналы инфракрасного диапазона. Если в сетке нет повреждений, то сигналы поступают на приемное устройство без искажений. Попытки по вреждения сетки приводят к обрывам или деформации кабелей, что

вызывает сигнал тревоги. Оптичес кие системы отличаются низким уровнем ложных тревог, вызванных воздействием на нее мелких животных, птиц, изменением погодных условий и высокой вероятностью обнаружения попыток вторжения. Следующим видом физической защиты является защита элементов зданий и помещений. Хорошую физическую защиту оконных проемов помещений обеспечивают традиционные металлические решетки, а также специальное остекление на основе пластических масс, армированных стальной проволокой. Двери и окна охраняемого помещения оборудуются датчика ми, срабатывающими при разрушении стекол, дверей, но не реагирующими на их колебания, вызванные другими причинами. Срабатывание датчиков вызывает сигнал тревоги. Среди средств физической защиты особо следует отметить средства защиты ПЭВМ от хищения и про никновения к их внутренним компонентам. Для этого используют металлические конструкции с клейкой подставкой, которая обеспечивает сцепление с поверхностью стола с силой в 2500 — 2700 кг/см. Это исключает изъятие или перемещение ПЭВМ без нарушения целостности поверхности стола. Перемещение ПЭВМ возможно только с использованием специальных ключей и инструментов.

Запирающие устройства

Запирающие устройства и специальные шкафы занимают особое место в системах ограничения доступа, поскольку они несут в себе признаки как систем физической защиты, так и устройств контроля доступа. Они отличаются большим разнообразием и предназначены для защиты документов, материалов, магнитных и фотоносителей и даже технических средств: ПЭВМ, калькуляторов, принтеров, ксероксов и других. Выпускаются специальные металлические шкафы для хранения ПЭВМ и другой техники. Такие шкафы снабжаются надежной двойной системой запирания: замком ключевого типа и трех — пятизначным комбинированным замком. Фирмы утверждают, что такие шкафы обладают прочностью и надежностью, доста точными для защиты от промышленного шпионажа. Выпускаются замки с программируемым временем открывания с помощью механических или электронных часов.

Системы контроля доступа

Регулирование доступа в помещения или здания осуществляется прежде всего посредством опознавания службой охраны или техническими средствами. Контролируемый доступ предполагает ограничение круга лиц, допускаемых в определенные защища емые зоны, здания, помещения, и контроль за пере движением этих лиц внутри них. Основанием допуска служит определенный метод опознавания и сравнения с разрешительными параметрами системы. Имеется весьма широкий спектр методов опознавания уполномоченных лиц на право их доступа в

помещения, здания, зоны. На основе опознавания принимается решение о до пуске лиц, имеющих на это право, или запрещение — для не имеющих его. Наибольшее распространение получи ли атрибутные и персональные методы опознавания. К атрибутным способам относятся средства подтверждения полномочий, такие, в частности, как документы (паспорт, удостоверение), карты (фотокарточки, карты с магнитными, электрическими, механическими идентификаторами и т. д.) и иные средства (ключи, сигнальные элементы и т.д.). Заметим, что эти средства в значительной мере подвержены различного рода подделками и мошенничеству. Персональные методы — это методы определения лица по его независимым показателям: отпечаткам пальцев, геометрии рук, особенностям глаз. Персональные характеристики бывают статические и динамические. К последним относятся пульс, давление, кардиограммы, речь, почерк и другие. Персональные способы наиболее привлекатель ные. Вопервых, они полно описывают каждого отдельного человека. Вовторых, невозможно или крайне трудно подделать индивидуальные характеристики. Статические способы включают анализ физических характеристик — таких, как отпечатки пальцев, особенности геометрии рук и другие. Они достаточно достоверны и обладают малой вероятностью ошибок. Динамические же способы используют изменяющиеся во времени опознавательные характеристики. Характеристики, зависящие от привычек и навыков, являются не только наиболее простыми для подделок, но и наиболее дешевыми с точки зрения практической реализации. Способы опознавания, основанные на чем-либо запоминаемом (код, пароль), могут применяться в слу чаях наиболее низких требований к безопасности, так как часто эта информация записывается пользовате лями на различных бумажках, в записных книжках и других носителях, что при их доступности другим может свести на нет все усилия по безопасности. Кроме того, имеется реальная возможность подсмотреть, подслушать или получить эту информацию другим путем (насилие, кража и т. д.). Способ опознавания человеком (вахтер, часовой) не всегда надежен из-за так называемого «человеческого фактора», заключающегося в том, что человек подвержен влиянию многих внешних условий (усталость, плохое самочувствие, эмоциональный стресс, подкуп). В противовес этому находят широкое приме нение технические средства опознавания, такие, на пример, как идентификационные карты, опознавание по голосу, почерку, пальцам и др. Простейший и наиболее распространенный метод идентификации использует различные карты и карточки, на которых помещается кодированная или открытая информация о владельце, его полномочиях и другое. Обычно это пластиковые карты типа пропусков или жетонов. Карты вводятся в читающее устройство каждый раз, когда требуется войти или выйти из охраняемого помещения или получить доступ к чему-нибудь (сейфу, камере, терминалу). Существует много разновидностей устройств опознавания и идентификации личности, использующих подобные карты.

Одни из них оптическим путем сличают фотографии и другие идентификационные элементы, другие — магнитные поля. Системы опознавания по отпечаткам пальцев. В основу идентификации положено сравнение относи тельного положения окончаний и разветвлений линий отпечатка. Поисковая система ищет на текущем изоб ражении контрольные элементы, определенные при исследовании эталонного образца. Для идентификации одного человека считается достаточным определение координат 12 точек. Эти системы, естественно, весьма сложны и реко мендуются к использованию на объектах, требующих надежной защиты. Системы опознавания по голосу. Существует не сколько способов выделения характерных признаков речи человека: анализ кратковременных сегментов, контрольный анализ, выделение статистических характеристик. Следует отметить, что теоретически вопросы идентификации по голосу разработаны достаточно полно, но промышленное производство пока налаже но слабо. Системы опознавания по почерку считаются наиболее удобными для пользователя. Основным принципом идентификации по почерку является постоянство подписи каждого индивидуума, хотя абсолютного совпадения не бывает. Система опознавания по геометрии рук. Для идентификации применяют анализ комбинации линий сгибов пальцев и ладони, линий складок, длины и толщины пальцев и других. Технически это реализуется путем наложения руки на матрицу фотоячеек. Рука освещается мощной лам пой, производится регистрация сигналов с ячеек, не сущих информацию о геометрии. Все устройства идентификации человека могут работать как отдельно, так и в комплексе. Комплекс может быть узкоспециальным или многоцелевым, при котором система выполняет функции охраны, контроля, регистрации и сигнализации. Такие системы являются уже комплексными. Комплексные системы обеспечивают: ♣ допуск на территорию предприятия по карточке (пропуску), содержащей индивидуальный машинный код; ♣ блокирование прохода при попытках несанкционированного прохода (проход без пропуска, проход в спецподразделения сотрудников, не имеющих допуска); ♣ возможность блокирования прохода для наруши телей графика работы (опоздание, преждевременный уход и т. д.); ♣ открытие зоны прохода для свободного выхода по команде вахтера; ♣ проверку кодов пропусков на задержание их предъявителей на КПП по указанию оператора системы; ♣ регистрацию времени пересечения проходной и сохранение его в базе данных персональной ЭВМ; ♣ обработку полученных данных и формирование различных документов (табель рабочего времени, суточный рапорт, ведомость нарушителей трудовой дисциплины и т. д.), что позволяет иметь опе ративную информацию о нарушителях трудовой дисциплины, отработанном времени; ♣ оперативную корректировку информации базы данных с доступом по паролю; ♣ распечатку табелей рабочего времени по произвольной группе сотрудников (предприятие в це лом, структурное подразделение, отдельно выбранные сотрудники); ♣ распечатку списков

нарушителей графика рабочего времени с конкретными данными о нарушении; ♣ текущий и ретроспективный анализ посещения сотрудниками подразделений, передвижения со трудников через КПП, выдачу списочного состава присутствовавших или отсутствовавших в подразделении или на предприятии для произвольно выбранного момента времени (при условии хранения баз данных за прошлые периоды); ♣ получение оперативной информации абонентами локальной сети в случае сетевой реализации сис темы. Физические средства являются первой преградой для злоумышленника при реализации им заходовых методов доступа.

2.3.3. Аппаратные средства защиты [^] К аппаратным средствам защиты информации относятся самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации. Аппаратные средства защиты информации применяются для решения следующих задач: ♣ проведение специальных исследований техничес ких средств обеспечения производственной дея тельности на наличие возможных каналов утечки информации; ♣ выявление каналов утечки информации на разных объектах и в помещениях; ♣ локализация каналов утечки информации; ♣ поиск и обнаружение средств промышленного шпионажа; ♣ противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям. По функциональному назначению аппаратные средства могут быть классифицированы на средства обнаружения, средства поиска и детальных измерений, средства активного и пассивного противодействия. При этом по своим техническим возможностям средства защиты информация могут быть общего на значения, рассчитанные на использование непрофессионалами с целью получения предварительных (общих) оценок, и профессиональные комплексы, позво ляющие проводить тщательный поиск, обнаружение и прецизионные измерения все характеристик средств промышленного шпионажа. В качестве примера первых можно рассмотреть группу индикаторов электромагнитных излучений типа ИП, обладающих широким спектром принимаемых сигналов и довольно низкой чувствительностью. В качестве второго примера — комплекс для обнаружения и пеленгования радиозак ладок, предназначенный для автоматического обнаружения и определения местонахождения радиопере датчиков, радиомикрофонов, телефонных закладок и сетевых радиопередатчиков. Это уже сложный современный поисково-обнаружигельный профессиональный комплекс. Таким является, например, комплекс «Дельта», который обеспечивает: ♣ достоверное обнаружение практически любых из имеющихся в продаже радиомикрофонов, радиостетоскопов, сетевых и телефонных передатчиков, в том числе и с инверсией спектра; ♣ автоматическое определение места расположения

микрофонов в объеме контролируемого помещенияПоисковую аппаратуру можно подразделить на аппа ратуру поиска средств съема информации и исследования: каналов ее утечки. Аппаратура первого типа направлена на поиск и локализацию уже внедренных зло умышленниками средств несанкционированного доступа Аппаратура второго типа предназначается для выявления каналов утечки информации. Примером такого комплекса может служи ть комплекс «Зарница», обеспечивающий измерение параметров побочных электромагнитных излучений в диапазоне частот от 10 Кгц до 1 Ггц. Обработка результатов измерений осуществляется на ПЭВМ в соответствии с действующими нормативно-методическими Документами Гостехкомиссии при Президенте РФ(рис. 19). Определяющими для такого рода систем являются оперативность исследования и надежность полу ченных результатов. Использование профессиональной поисковой аппаратуры требует высокой квалификации оператора. Как в любой области техники, универсальность той или иной аппаратуры приводит к снижению ее параметров по каждой отдельной характеристике. С другой стороны, существует огромное количество различных по физической природе каналов утечки информации, а также физических принципов, на осно ве которых работают системы несанкционированного доступа. Эти факторы обусловливают многообразие поисковой аппаратуры, а ее сложность определяет высо кую стоимость каждого прибора. В связи с этим доста точный комплекс поискового оборудования могут позволить себе иметь структуры, постоянно проводящие соответствующие обследования. Это либо крупные службы безопасности, либо специализированные фирмы, оказывающие услуги сторонним организациям. Конечно, описанное выше не является аргументом для отказа от использования средств поиска самостоятельно. Но эти средства в большинстве случаев до статочно просты и позволяют проводить профилактические мероприятия в промежутке между серьезными поисковыми обследованиями. В особую группу выделяются аппаратные средства защиты ЭВМ и коммуникационных систем на их базе. Аппаратные средства защиты применяются как в отдельных ПЭВМ, так и на различных уровнях и участках сети: в центральных процессорах ЭВМ, в их оперативных ЗУ (ОЗУ), контроллерах ввода-вывода, внешних ЗУ, терминалах и т. д. Для защиты центральных процессоров (ЦП) применяется кодовое резервирование — создание дополнительных битов в форматах машинных команд (разрядов секретности) и резервных регистров (в устройствах ЦП). Одновременно предусматриваются два возможных режима работы процессора, которые отделяют вспомогательные операции от операций непос редственного решения задач пользователя. Для этого служит специальная система прерывания, реализуемая аппаратными средствами. Одной из мер аппаратной защиты ЭВМ и информационных сетей является ограничение доступа к опе ративной памяти с помощью установления границ или

полей. Для этого создаются регистры контроля и регистры защиты данных. Применяются также дополнительные биты четности — разновидность метода кодового резервирования. Для обозначения степени конфиденциальности программ и данных, категорий пользователей исполь зуются биты, называемые битами конфиденциальности (это два-три дополнительных разряда, с помощью которых кодируются категории секретности пользователей, программ и данных). Программы и данные, загружаемые в ОЗУ, нуждаются в защите, гарантирующей их от несанкциони рованного доступа. Часто используются биты четнос ти, ключи, постоянная специальная память. При считывании из ОЗУ необходимо, чтобы программы не могли быть уничтожены несанкционированными действиями пользователей или вследствие выхода аппа ратуры из строя. Отказы должны своевременно выяв ляться и устраняться, чтобы предотвратить исполне ние искаженной команды ЦП и потери информации. Для предотвращения считывания оставшихся пос ле обработки данных в ОЗУ применяется специальная схема стирания. В этом случае формируется команда на стирание ОЗУ и указывается адрес блока памяти, который должен быть освобожден от информации. Эта схема записывает нули или какую-нибудь другую последовательность символов во все ячейки данного блока памяти, обеспечивая надежное стирание ранее загруженных данных. Аппаратные средства защиты применяются и в терминалах пользователей. Для предотвращения утеч ки информации при подключении незарегистрированного терминала необходимо перед выдачей запрашиваемых данных осуществить идентификацию (автоматическое определение кода или номера) терминала, с которого поступил запрос. В многопользовательском режиме этого терминала идентификации его недоста точно. Необходимо осуществить аутентификацию пользователя, то есть установить его подлинность и полномочия. Это необходимо и потому, что разные пользователи, зарегистрированные в системе, могут иметь до ступ только к отдельным файлам и строго ограниченные полномочия их использования. Для идентификации терминала чаще всего применяется генератор кода, включенный в аппаратуру терминала, а для аутентификации пользователя — такие аппаратные средства, как ключи, персональные кодовые карты, персональный идентификатор, устройства распознавания голоса пользователя или формы его пальцев. Но наиболее распространенными средствами аутентификации являются пароли, проверяемые не аппаратными, а программными средствами опознавания. Аппаратные средства защиты информации — это различные технические устройства, системы и сооружения, предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа.

2.3.4. Программные средства защиты [^]

Системы защиты компьютера от чужого вторжения весьма

разнообразны и классифицируются, как:

☐ средства собственной защиты, предусмотренные

общим программным обеспечением;

☐ средства защиты в составе вычислительной системы;

☐ средства защиты с запросом информации;

☐ средства активной защиты;

☐ средства пассивной защиты и другие.

Основные направления использования программной защиты информации Можно выделить следующие направления использования программ для обеспечения безопасности конфиденциальной информации, в частности такие: ♣ защита информации от несанкционированного доступа; ♣ защита информации от копирования; ♣ защита программ от копирования; ♣ защита программ от вирусов; ♣ защита информации от вирусов; ♣ программная защита каналов связи. По каждому из указанных направлений имеется достаточное количество качественных, разработанных профессиональными организациями и распространя емых на рынках программных продуктов (рис. 21). Программные средства защиты имеют следующие разновидности специальных программ: ♣ идентификации технических средств, файлов и аутентификации пользователей; ♣ регистрации и контроля работы технических средств и пользователей; ♣ обслуживания режимов обработки информации ограниченного пользования; ♣ защиты операционных средств ЭВМ и прикладных программ пользователей; ♣ уничтожения информации в защитные устройства после использования; ♣ сигнализирующих нарушения использования ресурсов; ♣ вспомогательных программ защиты различного назначения (рис. 22). Идентификация технических средств и файлов, осуществляемая программно, делается на основе ана лиза регистрационных номеров различных компонентов и объектов информационной системы и сопоставления их со значениями адресов и паролей, хранящихся в защитном устройстве системы управления. Для обеспечения надежности защиты с помощью паролей работа системы защиты организуется таким образом, чтобы вероятность раскрытия секретногопароля и установления соответствия тому или иному идентификатору файла или терминала была как можно меньше. Для этого надо периодически менять па роль, а число символов в нем установить достаточно большим. Эффективным способом идентификации адресуемых элементов и аутентификации пользователей яв ляется алгоритм запросно-ответного типа, в соответствии с которым система защиты выдает пользовате лю запрос на пароль, после чего он должен дать на него определенный ответ. Так как моменты ввода запроса и ответа на него непредсказуемы, это затрудняет процесс отгадывания пароля, обеспечивая тем самым более высокую надежность защиты. Получение разрешения на доступ к тем или иным ресурсам можно

осуществить не только на основе использования секретного пароля и последующих про цедур аутентификации и идентификации. Это можно сдела ть более детальным способом, учитывающим различные особенности режимов работы пользователей, их полномочия, категории запрашиваемых данных и ресурсов. Этот способ реализуется специальными программами, анализирующими соответствующие ха рактеристики пользователей, содержание заданий, параметры технических и программных средств, устройств памяти. Поступающие в систему защиты конкретные дан ные, относящиеся к запросу, сравниваются в процессе работы программ защиты с данными, занесенными в регистрационные секретные таблицы (матрицы). Эти таблицы, а также программы их формирования и обработки хранятся в зашифрованном виде и находятся под особым контролем администратора (администра - торов) безопасности информационной сети. Для разграничения обращения отдельных пользователей к вполне определенной категории информации применяются индивидуальные меры секретности этих файлов и особый контроль доступа к ним пользо вателей. Гриф секретности может формироваться в виде трехразрядных кодовых слов, которые хранятся в самом файле или в специальной таблице. В этой же таблице записываются идентификатор пользователя, создавшего данный файл, идентификаторы терминалов, с которых может быть осуществлен доступ к файлу, идентификаторы пользователей, которым разрешен доступ к данному файлу, а также их права на пользование файлом (считывание, редактирование, стирание, обновление, исполнение и т. д.). Важно не допустить взаимовлияния пользователей в процессе обращения к файлам. Если, например, одну и ту же запись имеют право редактировать несколько пользователей, то каждому из них необходимо сохранить именно его вариант редакции (делается несколько копий записей с целью возможного анализа и установления полномочий). Защита информации от несанкционированного доступа Для защиты от чужого вторжения обязательно предусматриваются определенные меры безопасности. Основные функции, которые должны осуществлять ся программными средствами, это: ♣ идентификация субъектов и объектов; ♣ разграничение (иногда и полная изоляция) досту па к вычислительным ресурсам и информации; ♣ контроль и регистрация действий с информацией и программами. Процедура идентификации и подтверждения подлинности предполагает проверку, является ли субъект, осуществляющий доступ (или объект, к которому осуществляется доступ), тем, за кого себя выдает. Подобные проверки могут быть одноразовыми или периодическими (особенно в случаях продолжительных сеансов работы). В процедурах идентификации используются различные методы. ♣ простые, сложные или одноразовые пароли; ♣ обмен вопросами и ответами с администратором; ♣ ключи, магнитные карты, значки, жетоны; ♣ средства анализа индивидуальных характеристик (голоса, отпечатков пальцев, геометрических параметров рук, лица); ♣ специальные идентификаторы или контрольные суммы для аппаратуры, программ, данных. Наиболее распространенным методом идентификации является парольная идентификация. Практика показала, что парольная защита данных является слабым звеном, так как пароль можно подслушать или подсмотреть, пароль можно перехватить, а то и просто разгадать. Для защиты самого пароля выработаны определен ные рекомендации, как сделать пароль надежным: ♣ пароль должен содержать по крайней мере восемь символов. Чем меньше символов содержит пароль, тем легче его разгадать; ♣ не используйте в качестве пароля очевидный набор символов, например ваше имя, дату рождения, имена близких или наименования ваших программ. Лучше всего использовать для этих целей неизве стную формулу или цитату; ♣ если криптографическая программа позволяет, введите в пароль по крайней мере один пробел, небуквенный символ или прописную букву;не называйте никому ваш пароль, не записывайте его. Если вам пришлось нарушить эти правила, спрячьте листок в запираемый ящик; ♣ чаще меняйте пароль, ♣ не вводите пароль в процедуру установления ди алога или макрокоманду. Помните, что набранный на клавиатуре пароль часто сохраняется в последовательности команд авто матического входа в систему. Для идентификации программ и данных часто прибегают к подсчету контрольных сумм, однако, как и в случае парольной идентификации, важно исключить возможность подделки при сохранении пра вильной контрольной суммы. Это достигается путем использования сложных методов контрольного суммирования

на основе криптографических алгоритмов. Обеспечить защиту данных от подделки (ими-тостойкость) можно, применяя различные методы шифрования и методы цифровой подписи на основе криптографических систем с открытым ключом. После выполнения процедур идентификации и установления подлинности пользователь получает доступ к вычислительной системе, и защита информации осуществляется на трех уровнях: ♣ аппаратуры; ♣ программного обеспечения; ♣ данных. Защита на уровне аппаратуры и программного обеспечения предусматривает управление доступом к вычислительным ресурсам: отдельным устройствам, оперативной памяти, операционной системе, специальным служебным или личным программам пользователя. Защита информации на уровне данных направлена: ♣ на защиту информации при обращении к ней в процессе работы на ПЭВМ и выполнении только разрешенных операций над ними; ♣ на защиту информации при ее передаче по каналам связи между различными ЭВМ. Управление доступом к информации позволяет ответить на вопросы: ♣ кто может выполнять и какие операции; ♣ над какими данными разрешается выполнять операции. Объектом, доступ к которому контролируется, может быть файл, запись в файле или отдельное поле записи файла, а в качестве факторов, определяющих порядок доступа, — определенное событие, значения данных, состояние системы, полномочия пользователя, предыстория обращения и другие данные. Доступ, управляемый событием, предусматривает блокировку обращения пользователя. Например, в определенные интервалы времени или при обращении с определенного терминала. Доступ, зависящий от состояния, осуществляется в зависимости от текущего состояния вычислительной системы, управляющих программ и системы защиты. Что касается доступа, зависящего от полномочий, то он предусматривает обращение пользователя к программам, данным, оборудованию в зависимости от предоставленного режима. Такими режимами могут быть «только читать», «читать и писать», «только выполнять» и другие. В основе большинства средств контроля доступа лежит то или иное представление матрицы доступа. Другой подход к построению средств защиты доступа основан на контроле информационных потоков и разделении субъектов и объектов доступа на классы конфиденциальности. Средства регистрации, как и средства контроля доступа, относятся к эффективным мерам защиты от несанкционированных действий. Однако, если средства контроля доступа предназначены для предотвращения таких действий, то задача регистрации — обнаружить уже совершенные действия или их попытки. В общем комплекс программно-технических средств и организованных (процедурных) решений по защите информации от несанкционированного доступа (НСД) реализуется следующими действиями: ♣ управлением доступом; ♣ регистрацией и учетом; ♣ применением криптографических средств; ♣ обеспечением целостности информации. Можно отметить следующие формы контроля и разграничения доступа, нашедшие широкое применение на практике: 1. Предотвращение доступа: a. к жесткому диску; b. к отдельным разделам; c. к отдельным файлам; d. к каталогам; e. к гибким дискам; f. к сменным носителям информации. 2. Установка привилегий доступа к группе файлов. 3. Защита от модификации: a. файлов; b. каталогов. 4. Защита от уничтожения: a. файлов; b. каталогов. 5. Предотвращение копирования: a. файлов; b. каталогов; c. прикладных программ. 6. Затемнение экрана по истечении времени, установленного пользователемЗащита от копирования Средства защиты от копирования предотвращают использование ворованных копий программного обеспечения и являются в настоящее время единственно надежным средством — как защищающим авторское право программистов-разработчиков, так и стимулирующим развитие рынка. Под средствами защиты от копирования понимаются средства, обеспечивающие выполнение программой своих функций только при опознании некоторого уникального некопируемого элемента. Таким элементом (называемым ключевым) может быть дискета, определенная часть компьютера или специальное устройство, подключаемое к ПЭВМ. Защита от копирования реализуется выполнением ряда функций, являющихся общими для всех систем защиты: ♣ идентификация среды, из которой будет запускать ся программа; ♣ аутентификация среды, из которой запущена программа; ♣ реакция на запуск из несанкционированной среды; ♣ регистрация санкционированного копирования; ♣ противодействие изучению алгоритмов работы системы. Под средой, из которой будет запускаться

программа, подразумевается либо дискета, либо ПЭВМ (если установка происходит на НЖМД). Идентификация среды заключается в том, чтобы некоторым образом поименовать среду с целью дальнейшей ее аутентификации. Идентифицировать среду — значит закрепить за ней некоторые специально созданные или измеренные редко повторяющиеся и трудно подделываемые характеристики — идентификаторы. Идентификация дискет может быть проведена двумя способами. Первый основан на нанесении повреждений на некоторую часть поверхности дискеты. Распростра ненный способ такой идентификации — «лазерная дыра». При таком способе дискета прожигается в некотором месте лазерным лучом. Очевидно, что сделать «« точно такую же дырку в дискете-копии и в том же самом месте, как и на дискете-оригинале, достаточно сложно. Второй способ идентификации основан на нестан дартном форматировании дискеты. Реакция на запуск из несанкционированной среды обычно сводится к выдаче соответствующего сообщения. Защита информации от разрушения Одной из задач обеспечения безопасности для всех случаев пользования ПЭВМ является защита информации от разрушения, которое может произойти при подготовке и осуществлении различных восстановительных мероприятий (резервировании, создании и обновлении страховочного фонда, ведении архивов информации и других). Так как причины разрушения информации весьма разнообразны (несанкционирован ные действия, ошибки программ и оборудования, компьютерные вирусы и пр.), то проведение страховочных мероприятий обязательно для всех, кто пользуется персональными ЭВМ. Необходимо специально отметить опасность компьютерных вирусов. Многие пользователи ЭВМ (ПЭВМ) о них хорошо знают, а тот, кто с ними еще не знаком, скоро познакомится. Вирус компьютерный — небольшая, достаточно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям. Вирус обычно создается для нарушения работы компьютера различ ными способами — от «безобидной» выдачи какого-либо сообщения до стирания, разрушения файлов. Основную массу вирусов создают люди, хулиганствующие программисты, в основном, чтобы потешить свое самолюбие или заработать деньги на продаже антивирусов. Антивирус — программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Такие программы бывают специализированными и универсальными. Чем отличается универсальный антивирус от специализированного? Специализированный способен бороться только с уже написанными, работающими вирусами, а универсальный — и с еще не написанными. К специализированным относится большинство антивирусных программ: AIDSTEST, VDEA TH, SERUM-3, ANTI-KOT, SCAN и сотни других. Каждая из них распознает один или несколько конкретных вирусов, никак не реагируя на присутствие остальных. Универсальные антивирусы предназначены для борьбы с целыми классами вирусов. По назначению антивирусы универсального действия бывают довольно различны. Широкое применение находят резидентные антивирусы и программыревизоры. И те и другие антивирусные программы обладают определенными возможностями, положительными и отрицательными (недостатки) характеристиками. Специализированные при своей простоте слишком узко специализированы. При значительном разнообразии вирусов требуется такое же многообразие антивирусов. Помимо использования в интересах защиты от вирусов антивирусных программ широко используют и организационные меры безопасности. Для уменьшения опасности вирусных актов возможно предпринять определенные действия, которые для каждого конкретного случая могут быть сокращены или расширены. Вот некоторые из таких действий: 1. Информировать всех сотрудников предприятия об опасности и возможном ущербе в случае вирусных атак. 2. Не осуществлять официальные связи с другими предприятиями по обмену (получению) программным обеспечением. Запретить сотрудникам приносить программы «со стороны» для установки их в системы обработки информации. Должны использоваться толь ко официально распространяемые программы. 3. Запретить сотрудникам использовать компьютерные игры на ПЭВМ, обрабатывающих конфиденциальную информацию. 4. Для выхода на сторонние информационные сети выделить отдельное специальное место. 5. Создать архив копий программ и данных. 6. Периодически проводить проверку контрольным суммированием или сравнением с

«чистыми» программами. 7. Установить системы защиты информации на особо важных ПЭВМ. Применять специальные антивирусные средства. Программная защита информации — это система специальных программ, включаемых в состав программного обеспечения, ре ализующих функции защиты информации.

2.3.5. Криптографические средства защиты

Криптография как средство защиты (закрытия) информации приобретает все более важное значение в мире коммерческой деятельности. Криптография имеет достаточно давнюю историю. Вначале она применялась главным образом в области военной и дипломатической связи. Теперь она необходима в производственной и коммерческой деятель ности. Если учесть, что сегодня по каналам шифрованной связи только у нас в стране передаются сотни миллионов сообщений, телефонных переговоров, огромные объемы компьютерных и телеметрических данных, и все это, что называется, не для чужих глаз и ушей, становится ясным: сохранение тайны этой пе реписки крайне необходимо. Что же такое криптография? Она включает в себя несколько разделов современной математики, а также специальные отрасли физики, радиоэлектроники, свя зи и некоторых других смежных отраслей. (Ее задачей является преобразование математическими методами передаваемого по каналам связи секретного сообщения, телефонного разговора или компьютерных данных таким образом, что они становится совершенно непонятными для посторонних лиц. То есть криптография должна обеспечить такую защиту секретной (или любой другой) информации, что даже в случае ее перехвата посторонними лицами и обработки любыми способами с использованием самых быстродействующих ЭВМ и последних достижений науки и техники, она не должна быть дешифрована в течение нескольких де сятков лет. Для такого преобразования информации используются различные шифровальные средства — такие, как средства шифрования документов, в том числе и портативного исполнения, средства шифрования речи (телефонных и радиопереговоров), средства шифрования телеграфных сообщений и передачи данных. Общая технология шифрования Исходная информация, которая передается по каналам связи, может представлять собой речь, данные, видеосигналы, называется незашифрованными сообщениями Р (рис. 24). В устройстве шифрования сообщение Р шифруется (преобразуется в сообщение С) и передается по «незакрытому» каналу связи. На приемной стороне сообщение С дешифруется для восстановления исходного значения сообщения Р. Параметр, который может быть применен для из влечения отдельной информации, называется ключом. В современной криптографии рассматриваются два типа криптографических алгоритмов (ключей). Это классические криптографические алгоритмы, основанные на использовании секретных ключей, и новые криптографические алгоритмы с открытым ключом, основанные на использовании ключей двух типов: секретного (закрытого) и открытого. В криптографии с открытым ключом имеются по крайней мере два ключа, один из которых

невозможно вычислить из другого. Если ключ расшифрования вычислительными методами невозможно получить из ключа зашифрования, то секретность информации, зашифрованной с помощью несекретного (открытого) ключа, будет обеспечена. Однако этот ключ должен быть защищен от подмены или модификации. Ключ расшифрования также должен быть секретным и защищен от подмены или модификации. Если, наоборот, вычислительными методами невозможно получить ключ зашифрования из ключа расшифрования, то ключ расшифрования может быть не секретным. Разделение функций зашифрования и расшифрования посредством разделения на две части дополни тельной информации, требуемой для выполнения опе раций, является той ценной идеей, которая лежит в основе криптографии с открытым ключом.

Технология шифрованна речи Наиболее распространенным способом шифрования аналогового речевого сигнала является разделе ние его на части. В этом случае входной речевой сигнал поступает в полосовые фильтры для выделения полос шифруемого спектра. Выходной сигнал каждого фильтра в процессе шифрования подвергается либо перестановке по частоте, либо перевороту спектра (инверсия), либо и тому и другому одновременно. Затем синтезируется полный шифровальный выходной сигнал. По этому принципу работает система AVPS (Analog Voice Prived System) — речевой шифратор (скремблер), который осуществляет перестановку отдельных «вырезок» входного сигнала с помощью полосового фильтра — анализатора. Система имеет 12 ключей шифрования, обусловленных возможными перестановками, что обеспечивает надежность используемого метода. Система AVPS используется в реальном времени с любыми унифицированными телефонами. Качество шифрования речи высокое, сохраняется узнаваемость абонента. Находят очень широкое распространение цифровые системы шифрования речевых сигналов. Эти системы обеспечивают высокую надежность шифрования. В системах шифрования данных используются в основном две элементарные системы: 1. Перестановка (биты или подблоки внутри каждого блока входных данных переставляются). 2. Замещение (биты или подблоки внутри каждого блока входных данных заменяются). Разработано большое число алгоритмов шифрования. К числу наиболее эффективных относится алго ритм DES (Data Encryption Standart) — стандарт шифрования данных. Американское национальное бюро по стандартизации NBS узаконило алгоритм DES в качестве стандарта для систем связи. Механизм шифрования в этом алгоритме основывается на использовании ключа длиной 56 бит. Для защиты промышленной и коммерческой информации на международном и отечественном рынкепредлагаются различные технические устройства и комплекты профессиональной аппаратуры шифрования и криптозащиты телефонных и радиопереговоров, деловой переписки и пр. Широкое распространение получили скремблеры и маскираторы, заменяющие речевой сигнал

цифровой передачей данных. Производятся средства защиты те летайпов, телексов и факсов. Для этих целей использу ются шифраторы, выполняемые в виде отдельных устройств, в виде приставок к аппаратам или встраиваемые в конструкцию телефонов, факс -модемов и других аппаратов связи (радиостанции и другие).

Аппаратные, программные, программно-аппаратные и криптографические средства реализуют те или иные услуги информационной безопасности различными механизмами защиты информации, обеспечивающими соблюдение конфиденциальности, целостности, полноты и доступности. Инженерно-техническая защита информации использует физические, аппаратные, программные и криптографические средств. Выводы 1. Комплексная безопасность информационных ресурсов достигается использованием правовых актов государственного и ведомственного уровня, организационных мер и технических средств за щиты информации от различных внутренних и внешних угроз. 2. Правовые меры обеспечения безопасности и за щиты информации являются основой порядка де ятельности и поведения сотрудников всех уровней и степени их ответственности за нарушения установленных норм и правил работы по обеспечению сохранности коммерческих секретов. 3. Организационные меры являются решающим звеном в формировании и реализации комплексных мер защиты информации. Они, в первую очередь, выражаются в создании службы безопасности коммерческого предприятия и обеспечении ее нормального функционирования. 4. Инженерно-техническая защита — это использование различных технических средств в интере сах обеспечения информационной безопасности

9. Защита информации ПРИ РАБОТЕ С ЗАРУБЕЖНЫМИ ПАРТНЕРАМИ

7.1. Направления взаимодействия с зарубежными партнерами [^] 7.1.1. Научно-техническое сотрудничество с зарубежными партнерами [^] В настоящее время бесспорен тот факт, что резулта ты созидательной интеллектуальной деятельности (новые технические и технологические решения, разработки, «ноу-хау» и т. д.) коллектива специалистов или отдельно го исследователя, разработчика являются товаром, кото рый может быть продан, куплен, обменен и украден. На сегодняшний день самые выгодные виды ин - теллектуального товара, которые достаточно широко продаются и покупаются — это программные продукты: программы, пакеты прикладных программ, системное программное обеспечение. Это связано с бурными темпами компьютеризации общества. Второе место занимают технологии — с целью их продажи со здаются специальные биржи; затем — изобретения, «ноу-хау», материалы экспертных оценок, банки и базы данных. Продажа и покупка остальных видов интеллектуального товара осуществляется нерегулярно, хотя в зарубежной практике дело обстоит иначе, например, достаточно перспективная научно-

техническая идея может быть украдена и в короткое время реализована в конкретном материальном продукте. В последние годы наблюдается активизация международного научно-технического сотрудничества. Участвуя в различных формах международного разделения и кооперации труда, российские предприниматели заключают многочисленные контракты, со глашения, договора. Выборочный анализ последних свидетельствует об отсутствии у российской стороны необходимых знаний и опыта по их составлению, в том числе в части вопросов, связанных с интеллектуальной собственностью. Результатом этого являются существенные экономические потери российской сторо- ны, которые находят свое конкретное отражение в: 1. потере всех прав, в том числе и патентных, вне территории стран СНГ (а иногда и на этой территории) на интеллектуальную собственность, впервые созданную или доведенную до практики при выполнении контракта (договора, соглашения); 2. в безвозмездной передаче в процессе выполнения соглашения принадлежащей ей интеллектуальной собственности; 3. блокировании процесса дальнейшего создания и коммерческого использования усовершенствований, самостоятельно разработанных ею после окончания срока действия контракта, соглашения, договора; 4. крайне заниженной цене контракта; 5. невозможности защитить принадлежащие российской стороне права в соответствии с российским судопроизводством. Это происходит вследствие: 1. отсутствия учета специфики российского рынка научных подрядчиков, представляющих собой, в основном, государственные научные организации с государственным финансированием, а следовательно, роли регулирования соответствующих отношений собственности со стороны правительства России; 2. использования только положений законодательных актов страны-партнера при отсутствии ссылок на соответствующие положения российского законодательства; 3. нарушения ряда положений российского законодательства, относящихся, в частности, к процедурам зарубежного патентования, экспортного контроля, договорным отношениям, недействительности договоров и т. д.; 4. отсутствия учета приносимого в процесс взаимодействия собственного интеллектуального вклада российской стороны; 5. чрезмерно широкого определения понятий «предмет соглашения», «изобретение», «право на использование», «совместный» и «собственный» (проприетарный) результат и других; 6. декларации действительности только иностранного текста контракта, а зачастую в отсутствии или неправильном переводе на русский язык раздела контракта, посвященного интеллектуальной собственности; 7. неучтенной стоимости передаваемых российской стороной патентных прав; 8. отсутствия механизма выявления нарушителей прав на объекты интеллектуальной собственности и мер, направленных на пресечение этих нарушений; 9. невыполнения ряда положений межправитель ственных соглашений в части, касающейся интеллектуальной собственности. Игнорирование вышеперечисленных

аспектов может привести к конфликтным ситуациям, подорвать доверие к процессу эффективного и взаимовыгодного сотрудничества. Составление соглашений (договоров) о сотрудничестве Одним из аспектов является правильное составление соглашений о совместном сотрудничестве, где необходимо точно определить тип соглашения (дого вора), которое имеет первостепенное значение, т. к. из него вытекают отношения сторон к правам на владение интеллектуальной собственностью. Преобладающими формами научно-технического взаимодействия между российскими и зарубежными организациями в настоящее время являются соглашения о научно-техническом сотрудничестве и договоры подряда. Между этими формами на практике неспециалисту трудно провести четкую грань. В ряде случаев они выступают как крайние формы правового взаимодействия партнеров, между которыми возможны самые различные варианты. Для соглашений о научно-техническом сотрудничестве характерно согласованное выполнение про граммы научноисследовательских, проектно-конструкторских и экспериментальных работ в целях достижения единого результата. По своему содержанию обязательства сторон в соглашениях о сотрудничестве — это взаимные обязательства по выполнению исследовательских и научно-технических работ. Важнейшим условием соглашения о сотрудничестве является наличие у партнеров общей хозяйственной цели (совместной деятельности по созданию и использованию результатов работы.) Поэтому обязательства сторон в соглашениях о сотрудничестве не противостоят друг другу, а являются общими, едиными. Для договоров подряда характерно, что одна сто рона (подрядчик) за установленную договором плату обязуется выполнить по заказу другой стороны (заказ чика) определенные в договоре подряда научно-технические работы и передать заказчику их результаты или оказать услуги научно-технического характера. У каждой из сторон такого договора имеются собствен ные (несовпадающие) интересы, в связи с чем их обя зательства носят встречный, противостоящий друг другу характер. Отражение в соглашениях вопросов интеллектуальной собственности 1) Интеллектуальная собственность в договорах подряда. Поскольку при проведении заказных работ творческий вклад в результирующую информацию вносится только одной стороной (подрядчиком), выполняющей работу за счет другой стороны (заказчика), в договорах подряда, как правило, не возникает совместных прав на владение объектами интеллектуальной собственности. Охранные документы в этом случае приобретаются либо на имя подрядчика, либо на имя заказчика. Определяющими критериями на практике выступают интеллектуальный и финансовый вклады сторон в создание интеллектуальной собственности. Независимо от того, на чье имя выданы охранные документы на объекты интеллектуальной собственно сти, патенты на изобретения, свидетельства на полезные модели и т. д., каждая из сторон имеет определенные права на использование интеллектуальной собственности, полученной в ходе

выполнения подрядных работ. 2) Интеллектуальная собственность в соглашениях о сотрудничестве. Полученные в ходе выполнения со глашений о сотрудничестве результирующая информация, результирующий патент, результирующее программное обеспечение, как правило, являются совместной (долевой) собственностью сторон. Доли участников долевой собственности устанавливаются соглашением сторон, а при его отсутствии признаются равными. Соглашением участников долевой собственности может быть установлен порядок определения и изменения их долей в зависимости от вклада каждого из них в образование и приращение общей собственности*. В соглашениях о сотрудничестве особое внимание следует уделить вопросам распределения прав на ре зультаты работ, полученные в рамках сотрудничества каждой из сторон, но не являющиеся конечным результатом сотрудничества, так называемые промежуточные результаты сотрудничества. Анализ мировой практики заключения соглашений в области международного научно-технического сотрудничества показывает, что большинство соглашений предусматривает, что каждая из сторон имеет право на неограниченное использование промежуточных результатов работ на территории своей страны. Для передачи таких результатов в третьи страны требуется согласие всех сторон соглашения. Доходы при этом распределяются между сторонами пропорционально зафиксированной в соглашении доле их участия. Защита интеллектуальной собственности Защита прав на совместные объекты интеллектуальной собственности от нарушений третьими лица ми должна осуществляться сторонами совместно либо по согласованию с партнером той стороной, которая вела работу по получению правовой охраны в стране, где нарушены соответствующие права. Меры по защите нарушенных третьими лицами прав на собственные изобретения в стране партнера, созданные сторонами в ходе сотрудничества и переданные друг другу для использования, должны быть четко определены в соглашении о сотрудничестве или договоре подряда. На практике возможны следующие варианты: 1. меры по защите нарушенных третьими лицами прав предпринимаются той стороной, которой та кие права принадлежат; 2. меры по защите нарушенных третьими лицами прав предпринимаются обеими сторонами; 3. меры по защите нарушенных третьими лицами прав предпринимаются тем партнером, в стране которого произошло нарушение указанных прав, ибо он обладает большими возможностями по организации защиты в своей стране. Аналогичным образом в соглашении следует определить процедуру защиты в случае предъявления в стране партнера претензий или исков со стороны третьих лиц. Соглашения и договоры подряда рекомендуется готовить на двух языках: русском и языке иностран ного партнера, сделав специальную оговорку в соглашении или договоре о том, что каждый из текстов имеет одинаковую юридическую силу. 7.1.2. Научно-техническое сотрудничество. Технологически и обмен и его регулирование. [^] Научно-техническое

сотрудничество — это процесс создания знаний и технологий, обмена ими, процесс, в котором результаты научно-технической деятельности выступают как специфический товар, имеющий потребительскую стоимость. Он разделяется на товар нематериальный: знания, навыки, методы; и материальный: оборудование, инструменты, оснастка и другое. Процесс обмена знаниями и технологиями формирует в самом общем виде рынок технологий с присущим ему инструментарием рыночных отношений. Объектами научно-технического сотрудничества и технологического обмена являются патенты на изобретения, промышленные модели и полезные образцы, «ноу-хау» (производственный опыт и знания), услуги (инжиниринг), техническая документация, техничес кая помощь, а также оборудование, машины и другая техника и технологии, в которых материализованы научно-технические знания. В Российской Федерации в настоящее время дей ствует пакет законов, регулирующих обмен технологиями и соответствующих аналогичным законам ведущих стран мира: Патентный закон; Закон «О товарных знаках, знаках обслуживания и наименования мест происхождения товаров»; Закон «О правовой охране программ ЭВМ и баз данных»; Закон «О правовой охране технологии интегральных схем» (приняты на Пятой сессии Верховного Совета Российской Федерации 23 сентября 1992 г.). Патентный закон РФ регулирует правовую охрану изобретений и промышленных образцов, при этом введена единая форма охранного документа — патент на изобретения и промышленные образцы и свиде тельство на полезную модель. Постановлением Правительства РФ от 12 июля 1993 г. № 648 установлен порядок использования изоб ретений и промышленных образцов, охраняемых действующими на территории Российской Федерации авторскими свидетельствами на изобретения и сви - детельствами на промышленный образец, и выплаты их авторам вознаграждения. Постановление распространяется на ранее выданные свидетельства СССР и устанавливает, что юридические лица, независимо от форм собственности, и физические лица, занимающиеся предпринимательской деятельностью, ис пользуют изобретения и промышленные образцы, охраняемые действующими на территории Россий ской Федерации авторскими свидетельствами СССР на изобретение и свидетельствами СССР на промышленный образец, без специального на то разрешения. Учитывая необходимость сохранения и развития научнотехнического потенциала и более широкого использования достижений науки и техники для структурных преобразований экономики России, государственное регулирование технологического обмена расширяет инструментарий стимулирования разработки и использования изобретений, промышленных образцов и полезных моделей за счет механизма льготного налогообложения и других льгот владельцам охранных документов. В частности, разработаны методы учета нематериальных активов (изобретений, полезных

моделей и других видов творческой деятельности), а также оценки интеллектуальной собственности в рамках сотрудничества (как правило, совместной деятельности) и перенесения их стоимости на издержки по со - вместной деятельности, что предполагает освобождение от налогов суммы общих затрат на совместную деятельность по доведению, к примеру, изобретения до конечного результата, оговоренного в документе, регулирующем сотрудничество (договор, контракт, соглашение). Рынок технологий Как и любой другой, рынок технологий имеет свою структуру, основными элементами которой являются товар, его производство и потребление, а также физические и юридические лица как субъекты рыночных отношений. Особенность технологии состоит в том, что она может выступать в качестве товара только в случае, если ее владелец обладает исключительным правом собственности на нее. Если же знания, лежащие в основе новой технологии, широко известны, то возможности получения коммерческих преимуществ от ее реализации отсутствуют, и, следовательно, становится невозможным и получение дополнительной прибы ли. Поэтому охрана права интеллектуальной собствен ности является неотъемлемым элементом рынка технологий. Международный технологический обмен играет существенную роль в современных мирохозяйствен ных связях. Это связано с тем, что развитие науки и техники, которое лежит в основе производства новых знаний, имеет глобальный характер, и знания легче, чем любой другой товар, пересекают национальные границы. В соответствии с методологией ООН, технология подразделяется на высокую, среднюю и низкую. Наи более мощным коммерческим потенциалом обладает высокая технология. Обмен ею приходится преимущественно на промышленно развитые страны. Средняя и низкая технологии для рынков этих стран практически не представляют коммерческой ценности, так как они широко распространены и их внедрение в большинстве случаев не создает условий для получения дополнительной прибыли. Средняя и низкая технологии обладают коммерческим потенциалом на рынках развивающихся стран, так как на уровне их научно-технического и экономического развития они обладают «новизной». Однако фирмы этих стран, освоив свои национальные рынки, сталкиваются с серьезными затруднениями при по пытках экспорта своей продукции, произведенной на основе этих технологий. Поэтому поток технологий по мере их старения направлен из более развитых к отстающим в своем развитии странам. Российским импортерам зарубежных технологий следует особенно внимательно относиться к оценке коммерческого по - тенциала приобретаемой технологии не только для внутреннего рынка, но и для будущего экспорта продукции, производимой с использованием этих технологий. Вместе с тем при продаже российских технологий за рубеж следует уделять особое внимание правильному выбору формы и способа передачи технологии. Ошибки в этой области ведут не только к существен ным

коммерческим потерям, но и к утрате научно-технического приоритета, лидерства в перспективе на мировых рынках. Участником технологического обмена может быть любое физическое или юридическое лицо, как индиви дуальное, так и коллективное (объединения, компании, фирмы, товарищества и ассоциации), а также любые их сочетания, независимо оттого, кем они были созданы, кому принадлежат, кем контролируются (государ ством, правительственными учреждениями, юридическими лицами или отдельными гражданами), где функционируют, и независимо от форм собственности. Под потребителем технологии подразумевается сторона, которая получает право (лицензию) на ис пользование или эксплуатацию технологии, носящей патентный или не патентный характер, покупает или каким-либо иным образом приобретает технологию или право на нее. Под поставщиком технологии подразумевается сторона, которая предоставляет, продает, передает или каким-либо иным образом поставляет технологию, носящую патентный или не патентный характер, или право на нее. Существует несколько путей технологического обмена. Наиболее распространено разделение потока технологического обмена на коммерческие и некоммерческие, международные, внутригосударственные и внутрифирменные варианты передачи технологии. К некоммерческим вариантам технологического обмена относятся: ■ свободное распространение научно-технической информации (научно-технической, учебной лите ратуры, справочников, обзоров, стандартов, описаний патентов, каталогов, проспектов и т. д.); ■ обмен информацией в ходе международных конференций, сессий, симпозиумов и выставок; ■ научный обмен, обучение и стажировка ученых и специалистов на бесконтрактной основе или на ус ловиях паритетного возмещения расходов сторонами. По каналам некоммерческого обмена чаще всего проходит передача технологий в области научных ис следований фундаментального характера. Обмен технологией по некоммерческим каналам обычно сопровождается небольшими расходами, в том числе валютными. Он может осуществляться как по государственной линии, так и частным образом на основе личных контактов. Передаче технологий прикладного характера боль ше соответствуют коммерческие каналы, по которым в форме сделок осуществляются: ■ продажа или предоставление по лицензии всех форм промышленной и интеллектуальной собственности; ■ передача «ноу-хау» и технического опыта в виде технико-экономических обоснований, планов, ди аграмм, моделей, образцов, инструкций, руко водств, формул, сборочных или рабочих чертежей, спецификаций, технологической оснастки и инструмента, услуг консультантов и подготовки кадров; ■ передача технических знаний, необходимых для монтажа, эксплуатации предприятий, цехов и оборудования, а также проектов по строительству объектов «под ключ»; ■ предоставление технологических знаний в рамках соглашений о совместной научно-технической деятельности, совместном производстве и сбыте;

контрактов на приобретение и монтаж машин, оборудования, полуфабрикатов или сырьевых материалов или их аренду (лизинг). На рынке технологий действует сеть покупателей и продавцов, соединенных посредническими звеньями инновационной инфраструктуры. В обобщенном виде она складывается из следующих элементов: ■ исследовательских, внедренческих и инновацион ных форм и компаний, университетов и учрежде ний, предлагающих результаты своих разработок; ■ бирж, торговых домов, ярмарок, аукционов, магазинов и других мест совершения сделок, которые специализируются на определенных видах прода ваемых знаний; ■ посреднических компаний, предоставляющих профессиональные услуги продавцам и покупателям технологии (инжиниринговых, консульта ционных, аудиторских, лизинговых, информационных и других). ■ фондов рискового капитала, кредитных учрежде ний и банков; ■ национальных, региональных и международных информационных центров, снабжающих всех участников купли-продажи конкретного вида технологии информацией, в том числе и о зарубежных рынках; ■ региональных и национальных союзов и консорциумов, холдингов и т. д., содействующих развитию рынков конкретных видов технологии. 7.1.3. Виды коммерческих международных операций [^] Объектами международных коммерческих операций являются материально-вещественная продукция и услуги, включая результаты производственного и на учно-технического сотрудничества, приобретающие в обмене форму товара. Эти объекты определяют виды коммерческих операций, осуществляемых на мировом рынке. Международные коммерческие операции подразделяются на основные, осуществляемые на безвозмездной основе между непосредственными участниками этих операций (контрагентами разных стран), и обеспечивающие, связанные с продвижением товара от продавца к покупателю. К основным коммерческим операциям относятся операции: ■ по обмену научно-техническими знаниями (в форме торговли патентами, лицензиями, «ноу-хау»); ■ по обмену техническими услугами (консультатив ный и строительный инжиниринг); ■ технологический обмен; ■ по предоставлению консультационных услуг в области информации и совершенствования управ ления. Осуществление международных операций требует применения определенных правовых форм и использования конкретных методов их проведения. Правовой формой, опосредствующей международные коммерческие операции является международная торговая сделка, обязательное условие которой — заключение ее иностранным контрагентом. Под международной торговой сделкой понимается договор (соглашение) между двумя или несколькими сторонами, находящимися в разных странах по поставке установленного количества товарных единиц и/или оказания услуг в соответствии с согласованными сторонами условиями. Международный характер договора вытекает из того, что его субъектами (сторонами) являются коммерческие предприятия (фирмы),

находящиеся в разных странах. Договор купли -продажи не будет считаться международным, если он заключен между сторонами разной государственной (национальной) принадлежнос - ти, коммерческие предприятия (фирмы) которых находятся на территории одного государства (например, между филиалами и дочерними компаниями фирм разных стран, находящихся на территории одной страны). В то же время договор признается международным, если он заключен между сторонами одной государственной (национальной) принадлежности, коммерческие предприятия которой находятся на тер ритории разных государств. Такое толкование договора содержится в конвен ции ООН о договорах международной купли-продажи товаров (Венская конвенция 1980 года) и в Новой гаагской Конвенции о праве, применимом к договорам международной купли-продажи 1985 года. Основные виды международных коммерческих операций можно охарактеризовать кратко следующим образом. Операции по торговле научно-техническими знаниями (опытом) отличаются от операций по торговле материальными ценностями тем, что предметом международного обмена в них выступают результаты де ятельности, которые принято считать «невидимым» товаром. Операции по торговле научно-техническими знаниями связаны с обменом результатами производственных научных исследований и разработок, имеющих не только научную, но и коммерческую ценность. В качестве товара здесь выступают продукты интеллектуального труда, облеченные в форму патентов, ли цензий, товарных знаков, промышленных образцов, представляющих собой часть так называемой промышленной собственности, а также технические знания и опыт, объединяемые понятием «ноу -хау», включающих передачу знаний и опыта путем предоставления технической документации, чертежей, секретов производства, не подлежит патентованию. Научно-технические знания поступают в между народный оборот либо на основе купли-продажи (при продаже патентов), либо — отношений, возникающих в связи с получением временного права пользования результатами на базе международных лицензионных соглашений. Операции по обмену лицензиями состоят в предоставлении права (разрешения) одной стороной — патентовладельцем, именуемым лицензором, другой стороне — лицу (или фирме), именуемому лицензиатом, на промышленное и коммерческое изобретения, пользующегося патентной защитой в течение обусловленного срока за определенное вознаграждение. Предоставление иностранному контрагенту ли цензий на использование изобретений, технических знаний и опыта, а также товарных знаков называется заграничным лицензированием. Операции по торговле техническими услугами, получившими в международной практике название инжиниринговых. Как самостоятельный вид международных коммерческих операций инжиниринг предпо лагает предоставление на основе договора на инжиниринг одной стороной, именуемой консультантом, другой стороне, именуемой заказчиком, комплекса или

отдельных видов инженерно-технических услуг, связанных с проектированием, строительствам и вводом объекта в эксплуатацию; с разработкой новых техноло гических процессов на предприятия заказчика; усовершенствованием имеющихся производственных процес сов вплоть до внедрения изделия в производство. Предоставление на основе договора на инжини ринг полного комплекса услуг и поставок, необходимых для строительства нового объекта, называется комплексным инжинирингом. Он включает три отдельных вида инженерно-технических услуг, каждый из которых может быть предметом самостоятельного договора: ■ консультативный инжиниринг, связанный глав ным образом с интеллектуальными услугами в целях проектирования объектов, разработки и планов строительства и контроля за проведением работ; ■ технологический инжиниринг, состоящий в предоставлении заказчику технологии или технологий, необходимых для строительства промышленного объекта и его эксплуатации (договоры на передачу производственного опыта и знаний), разработки и планов строительства и контроля за проведением работ; ■ строительный и/или общий инжиниринг, состоящий главным образом в поставках оборудования, техники и/или монтажа установок, включая в случае необходимости инженерные работы. Инже нерноконсультационные услуги предоставляются в виде технической документации, результатов исследований, исходных данных для строитель ства, экономических расчетов, смет, рекомендаций и т. д. В этой работе следует руководствоваться разработанным (в 1982 г.) группой экспертов по международным договорам на поставку промышленной продукции Комитета по развитию торговли ЕЭК ООН «Руководством по составлению международных договоров на консультативный инжиниринг, включая связанные с этим аспекты технического содействия». Оно содержит подробный перечень и характеристику условий, необ - ходимых для включения в договор между консультан том и заказчиком, а также перечень услуг, предостав ляемых инженеромконсультантом. В него включаются, в частности, следующие услуги: ■ проведение предварительных технико-экономических обоснований и исследований, связанных с общим проектированием; ■ планирование и подготовка чертежей и смет рас ходов; ■ подготовка предварительных эскизов, проектной документации, детальных чертежей и специфика ций; ■ планирование и составление программы финансирования; ■ подготовка технических условий для участия в торгах и выдача рекомендаций по поступающим предложениям; ■ оценка предложений о строительстве объектов; ■ контроль за строительством, изготовлением оборудования, монтажом, наладкой и пуском оборудования в эксплуатацию; ■ выдача сертификатов о качестве проведенных работ и других. Сотрудничество по реализации коммерческих операций международного производственно го и научно-технического сотрудничества зарубежных фирм выступает как результат определенной организационно -управленческой

деятельности, целью которой является заключение соглашений: ■ о специализации и кооперировании производства; ■ об организации совместного строительства объектов и их эксплуатации; ■ о поставке крупных промышленных объектов с компенсацией (оплатой) товарной продукции; ■ о кооперации в области научных исследований и других. Реализация этих соглашений осуществляется на основе заключения международных коммерческих сделок. Поэтому область производственного и научно-технического сотрудничества входит в сферу между народной торговли. Из анализа совместной деятельности с зарубежными представителями, очевидно то, что любые соглашения между двумя фирмами (компаниями) заключаются при непосредственном контакте, т. е. на официальных встречах, переговорах. Любая договоренность о сотрудничестве оформляется соответствующими договорами. Хотя одним из наиболее важных условий, исполь зуемых в международной практике, при заключении подобного рода договоров является условие об обеспечении защищенности информации в отношении предмета договора, без включения такого условия нельзя сохранить существенный элемент сделки — конфиденциальность. Такое условие должно включать в себя следующее: 1. взаимное обязательство сторон принимать все необходимые меры для предотвращения разгла шения коммерческой тайны с перечислением основных мер; 2. документы или изделия, указанные в договоре, будут рассматриваться сторонами как строго конфиденциальные; 3. стороны берут на себя обязательства принимать все необходимые меры для предотвращения нару шений правил пользования этими документами или изделиями, установленных в соответствующих статьях договора; 4. стороны обязуются не передавать без предварительного согласия другой стороны оригиналы документов или изделий, их копии или репродукции любого рода третьим сторонам; 5. стороны обязуются обеспечить ознакомление с информацией, составляющей коммерческую тайну предмета договора, только лишь строго ограниченного числа своих работников, с которых должны быть взяты подписки о неразглашении информации, составляющей коммерческую тайну, содержащейся в предмете договора или являющейся предметом договора. Нарушение такого рода требований договоров может привести к его аннулированию и привлечению виновников к ответственности в соответствие с действующим законодательством. 7.1.4. Научно-техническая документация - источник конфиденциальной информации [^] В состав научно-технической документации входят: ■ научно-исследовательская (научная), конструкторская, технологическая, проектная и другая произ водственная документация; ■ кино-фотодокументы, документы на машиночитаемых носителях: —документы по изобретениям и открытиям; — геолого-геодезические, метеорологические, экологические и другие документы. Научно-технические документы в зависимости от способа их выполнения и характера использования подразделяются на оригиналы, подлинники, дублика ты,

копии и эскизы. Виды научно-технических документов 1. Научно-исследовательская (научная) документация: a. итоговые и этапные отчеты о НИР и ОКР; b. технические отчеты; c. заключения, отзывы и рецензии; d. аннотации, паспорта, регламенты; e. монографии, диссертации и отзывы на них; f. рукописи неопубликованных научных работ; g. рекомендации различного характера; h. технические задания на НИР, ОКР; i. программы НИР; j. технико-экономические обоснования, обзоры, доклады; k. первичная документация в процессе НИР, ОКР, ОТР и ЭПР (ОТР — опытно-технологическая, ЭПР — экспертно-проектная): журналы записей, экспериментов, различных анализов; дневники; кино-фотодокументы; документы на машинных носителях. 2. Конструкторская документация (КД) — это совокупность графических и текстовых конструкторских документов, которые самостоятельно или в совокупности определяют состав и устройство изделия и содержат необходимые данные для его разработки или изготовления, контроля, приемы эксплуатации и ремонта. Включает: a. технические предложения; b. эскизные проекты; c. технические проекты; d. рабочую конструкторскую документацию. 3. Технологическая документация (ТД) — это сово- купность графических и текстовых технологических документов, которые самостоятельно или в совокупности определяют технологический процесс изготовле ния изделий промышленного производства или процесс сооружения объектов капитального строительства. 4. Проектная документация (ПД) — это совокупность технических документов, фиксирующих процесс и результаты проектирования. 5. Документы автоматизированных систем обработки данных и автоматизированных систем проектирования. Критерии ценности НЦ На каждом этапе экспертизы ценности НТД применяется в комплексе система общих и специфических критериев. К общим относятся критерии: ■ происхождение: организация, роль и место органи зации в системе организаций страны или в конкретной отрасли; значимость выполняемых ею функций; время и место создания; авторство документов. ■ содержание: значимость проблемы и объекта, отраженного в документах; значение содержащейся в документах информации, ее повторение в других документах; целевое назначение, вид и разно видность документа. ■ внешние особенности: юридическая содержатель ность документа — наличие подписей, дат, печатей; наличие резолюций, помет; особенности передачи документа, текста, подлинность; особенности материальной основы документа; особенности физичес кого состояния, полноты, сохранности документа. К специфическим относятся критерии: ■ принципиальная новизна, уникальность, ориги нальность решения проблемы, конструкции, технологии, проекта; ■ степень о тражения уровня науки и техники, про изводства на данном этапе развития общества; ■ значимость проблемы, проекта, модели, конструкции, технологии на момент внедрения для разви тия конкретных отраслей производственной и хо зяйственной деятельности; ■ экономическая

эффективность внедрения резуль татов исследования или технической идеи; ■ социальная эффективность исследования или раз работки. 7.1.5. Возможные условия разглашения сведений, составляющих коммерческую тайну [^] По мере развития рыночных отношений и расширения внешнеэкономических связей российских фирм у иностранных партнеров и конкурентов все чаще появляются устремления к сведениям о планах фирмы, ее финансовом положении, методах управления, рыночной стратегии. Возникновение конкуренции также порождает между ними подобные устремления. Построение системы защиты коммерческой тайны фирмы более чем необходимо при регулярном сотрудничестве с иностранными представителями. По строение такой защиты целесообразно начать с определения открытых источников и соответствующих им возможных официальных каналов распространения конфиденциальной информации. С учетом специфики научно-технической и коммерческой деятельности, степенью развития связей с деловыми партнерами хотелось бы выделить перечень официальных каналов передачи информации при таком взаимодействии: ■ выступления сотрудников фирмы с докладами и в дискуссиях на международных конференциях и симпозиумах, проводимых в России и за рубежом; ■ передача информации в процессе общения с иностранными журналистами; ■ демонстрация научно-технических фильмов; ■ демонстрация действующих объектов научно-технических достижений (оборудования, изделий, технологии); ■ демонстрация научно-технических достижений на выставках, проводимых в России и за рубежом; ■ все виды рекламы экспортной продукции в форме печатных изданий — брошюр, стендовой литературы для выставок и ярмарок; ■ обмен с зарубежными научными учреждениями, предприятиями и фирмами отчетами о НИОКР в соответствии с соглашениями о научно-техническом сотрудничестве или о совместном выполнении исследования и разработок; ■ публикация научных, технических и других мате риалов в зарубежных и международных изданиях; ■ передача информации при переписке с зарубежными научными учреждениями и специалистами; ■ передача сведений представителям иностранных фирм в процессе переговоров или при заключе нии экспертных или импортных соглашений; ■ прием иностранных специалистов на территории фирмы; ■ проведение совместных разработок (проектов, экспериментов) в рамках осуществления научнотехнических связей. Каждый из вышеуказанных каналов характеризуется весьма значительными объемами передачи информации зарубежными партнерами. Анализ, поступающих по открытым каналам сведений позволяет иностранным экспертам получать сообщения о деятельности фирмы, ее достижениях и другую ценную информацию. Для сбора интересующей информации зарубежные фирмы активно используют различные приемы добывания информации особенно на международных выставках. Путем опроса и анкетированная российских специалистов получают подробную

информацию об их месте работы, тематике проводимых ими иссле - дований и разработок. Основным «производителем» и «держателем» информации является человек. Это первичный ка нал как возникновения, так и утраты любого объекта интеллектуальной собственности. Исходя из этого основное внимание должно быть уделено сотрудни кам фирмы, начиная от момента их поступления на работу. Миграция специалистов, особенно имевших дело с конфиденциальной информацией, — самый основной и трудно контролируемый канал утечки информации. Так, получившая у нас в последнее время широкое распространение практика разного рода совместительства сотрудников, прежде всего научноисследовательских организаций, где они используют свои профессиональные знания, опыт и навыки, приобретенные по основному месту работы, т. е. фактически интеллекту альный продукт организации, только должным образом не оформленный в ее собственность, является одним из наиболее вероятным каналом утечки информации. По опыту зарубежных стран и после увольне - ния сотрудника (по крайней мере, в течение года) внимание к его дальнейшей деятельности не должно ослабевать. Особыми каналами утраты интеллектуальной собственности или, по крайней мере, ее коммерческой ценности являются совместные работы с другими фирмами, контакты с клиентами и инвесторами, где особое место занимают переговоры. (Так, например, в целях сбора интересующей их информации инофирмы нередко идут на создание совместных предприятий.) Не следует упускать из виду также технические средства недобросовестной конкуренции (промышленного шпионажа), которые все чаще проникают и на наш внутренний рынок. Тем более, что многие производственные процессы сопровождаются явлениями, имеющими физическую, химическую, биологическую и иную природу, в результате которых переносится та или другая информация. Анализ и обобщение возможных путей утраты интеллектуальной собственности (следовательно, и мероприятий по их перекрытию) должны вестись по следующим основным направлениям: 1. Люди. 2. Документы. 3. Изделия — процессы. Учитывая большое количество и разнообразие конкретных каналов утечки информации, наиболее целесообразным является построение работы именно исходя из перечисленных направлений. Разработку мероприятий по сохранению коммерческой тайны предприятия следует осуществлять, соблюдая принцип комплексного перекрытия возможных кана лов утечки информации и обеспечения равнозначной надежности защиты всех ее носителей. Защита от утечки конфиденциальной информации полностью ложится на саму фирму. Необходимо самим постоянно проявлять заботу о защите собственных передовых технологий, новых научных идей и результатов перспективных разработок. Це - лесообразно задерживать публикации о полученных научных результатах, выхолащивать из них сведения, представляющие интерес для научной общественности, ограничивать доступ к ней широкого круга лиц. В

процессе проведения совместных встреч, где обстановка общения, характеризующаяся сравнительно большим количеством участников, присутствием посторонних лиц, необходимостью придать огласке конфиденциальную информацию, сложностью контроля за поведением участников и т. п., объективно создают условия повышенной уязвимости информации. Следовательно, все это ставит организацию перед необходимостью принятия мер по защите собственных информационных ресурсов, в процессе реализации которых решаются задачи в совокупности по следую щим направлениям: ■ отбор и группировка информации, подлежащей ог лашению; ■ разработка и реализация правил проведения со вещаний и переговоров, приема посетителей; ■ организация работы с персоналом, т. е. лицами, которым поручена организация и проведение со вещаний и переговоров, ответственными за прием посетителей; ■ проведение мероприятий по обеспечению требований, предъявляемых к помещениям, где проводятся совещания и переговоры; их охрана. 7.1.6. Экспертиза ценности передаваемой научнотехнической документации [^] Экспертиза ценности конструкторской документации Экспертизе подвергаются: ■ на стадии «эскизный проект» — ведомости эскизного проекта и пояснительные записки; ■ на стадии «технический проект» — чертежи общих видов изделий; ведомости технического проекта; пояснительные записки; патентный формуляр; карты технического уровня и качества продукции; технико-экономические показатели; ■ на стадии «рабочая документация» — сборные чертежи изделия; габаритные и монтажные чертежи, схемы, технические условия, расчеты экономической эффективности изделия, спецификации, акты (государственных, отраслевых, фирменных) испыта ний и приемки изделия, групповые конструкторские чертежи; кино-фотодокументы, отражающие процесс обработки, изготовления и испытания изде лия; спецификации по видам обеспечения; инструкции по ведению массивов данных в АС ОД и САПР; каталоги баз данных, тексты программ, описания языков; положения о службе САПР и другие. Экспертиза ценности технологической документации Экспертизе подвергаются: ■ технологические документы, отражающие новые технологические процессы, методы организации производства и труда, экономии материалов; ■ чертежи универсального технологического оснащения для механической обработки деталей, сборки изделий, которые могут применяться для не скольких изделий, цехов, предприятий; ■ документация по технологической оснастке, отличающаяся новизной и совершенством конструкции; ■ технические документы на приспособления для совершенствования технологических процессов. Особое внимание уделяется экспертизе таких до кументов как: ■ маршрутные карты, технологические инструкции, правила, рецептура, описания, диаграммы, характеристики, схемы, режимы производства, ведомости технологической оснастки, карты основных и типовых технологических процессов, карты уровня

аттестуемой продукции, регламенты; ■ технические условия на изготовление изделий основного производства, альбомы технологических процессов, чертежей измерительных и контрольных приборов и инструментов; ■ технико-экономические показатели, нормы расхо дов материалов, технологические паспорта, спе цификация основного технологического оборудования. Экспертиза ценнпсти приемной документации Экспертизе подвергаются: ■ задания на проектирование продукции, проекты размещения строительства, проекты планировки, отчеты об изысканиях, генеральный план, ситуационный план, общая (сводная) пояснительная записка, схемы и описания технологических про цессов и оборудования, основные чертежи архитектурно-строительной части, чертежи цехов, фотографии общего вида зданий, корпусов и цехов, чертежи уникального характера; планы расположения зданий, транспортных путей, подземных сетей и ограждений; планы размещения оборудования, генеральные сметы к проектам реконструкции, сметно-финансовые расчеты.

10. Методы и средства защиты информации.

7.1. Технологии идентификации человека

7.2. Применение паролей в механизме аутентификации человека

7.3. Информационная безопасность компании

Для защиты информации при помощи устройств применяются три основных класса контроля доступа. К ним относятся: 1) контроль, основанный на обладании (ключи); 2) контроль, основанный на личных характеристиках (биометрические приборы); 3) контроль, основанный на знании (пароли). В случае контроля, основанного на обладании, речь идет о предметах, принадлежащих пользователю, - физическом ключе, магнитной карте и т.д. Биометрические приборы анализируют специфические физические особенности пользователя (подпись, отпечатки пальцев или рисунок линий на ладони) и сравнивают их с теми, что наличествуют у них в памяти. Последний вид контроля над доступом, наиболее распространенный, основан на обладании специфической информацией. Это означает, что правом доступа обладают лишь те лица, которые способны продемонстрировать свое знание определенного секрета, обычно пароля. Меры контроля доступа должны обеспечить две вещи. Вопервых, человек должен попасть в систему, а во-вторых, система должна оставить других снаружи. Независимо от того, какая система защиты используется, чаще всего первым шагом работы является идентификация и аутентификация пользователя: кто вы такой и можете ли доказать, что вы это вы? Идентификация - отождествление, установление соответствия одной сущности

другой._____ Аутентификация - совокупность процедур, цель которых - доказательство того, что идентифицированная сущность является именно той, за которую она себя выдает. Пользователь идентифицируется именем (идентификатором), а потом аутентифицируется паролем (или другим признаком аутентификации). Как только информационная система (компьютер) узнает вас, он сможет выяснить, что вам разрешено и чего не позволено делать. 7.1. Технологии идентификации человека Технологии идентификации человека в истории. Идентификация по фотографии. Идентификация по отпечаткам пальцев. Идентификация по ДНК. Компьютерная биометрия. Уязвимость биометрических систем. Технологии идентификации человека в истории В 1563 году книге «Сочинения об Азии» исследователь Хоайо де Баррос описывал как китайские торговцы «паспортизировали» детей, делая отпечатки их ладоней и ступней при помощи бумаги и чернил. При раскопках в Израиле археологи обнаружили наборы глиняной посуды, на каждом предмете отчетливо видны отпечатки больших пальцев, которые гончар использовал как персональное клеймо. В литературе можно найти много примеров ошибочной идентификации: «Принц и нищий» Марка Твена, пьесы Шекспира. Эти истории дошли до наших дней, потому что такого рода ошибки были редкостью. В Европе фамилии не использовались вплоть до Средневековья и вплоть до промышленной революции в мире не было нужды в системе точной идентификации. Развитие крупных городов и наплыв иммигрантов во второй половине XIX века для правительств многих стран превратилось в серьезную проблему. В Европе и США принимались жесткие иммиграционные законы, призванные сократить приток иностранцев, что потребовало создания системы точной идентификации, которая позволяла бы властям отличать граждан от неграждан. Система идентификации нужна была и для отделения рецидивистов от совершивших преступление впервые. Кроме этого, требовалась новая концепция реабилитации преступников, предоставлявшая возможность людям, совершившим ранее преступления, реабилитироваться и встать на путь исправления. Проблема идентификации осужденных привлекла внимание парижского антрополога А. Бертильона (1853-1914 гг.). Он заметил, что, даже если человек назовется другим именем, сменит прическу, наберет вес, некоторые части его тела останутся неизменными. Он создал систему антропологического опознавания, базирующуюся на этих неизменных признаках. Производились точные измерения головы, рук, ступней и ушей подозреваемого, фиксировалось наличие шрамов, родимых пятен, другие отличительные телесные признаки. Эта информация вместе с именем подозреваемого заносилась в специальные карты, которые затем хранились в центральном полицейском участке. Система Бертильона стала вехой в развитии криминалистики. Человек мог быть арестован и описан в 1881 году одним полицейским и опознан три года спустя другим полицейским в результате

обнаружения совпадения признаков после просмотра картотеки. Бертильон создал систему, позволяющую идентифицировать человека по записям, в то время как ранее это мог сделать только человек с хорошей зрительной памятью. В течение десяти лет после официального принятия указанной системы в декабре 1882 года парижская полиция выявила 4564 человека, назвавших полиции вымышленное имя. Система Бертильона дала возможность французским судьям выносить более жесткие приговоры рецидивистам. Буквально через несколько лет уровень преступности в Париже снизился. Бертильон объяснял это тем, что карманники сочли за лучшее мигрировать в места, где шанс их идентификации был ниже. Идентификация по фотографии Сегодня наиболее распространенной формой идентификации является помещение фотографии на официальный документ. Повсюду в мире универсальным способом идентификации личности является паспорт. Во многих европейских странах паспорт дополняется идентификационной карточкой. Надёжность идентификационных удостоверений (например, водительских) зависит от двух факторов. Во-первых, нужно быть уверенным, что удостоверение выдано соответствующему лицу. Во-вторых, само по себе удостоверение должно быть хорошо защищено от подделки. Удостоверения, которые легко подделать, провоцируют преступления, т.к. удостоверение может быть украдено, изменено и затем использовано в преступных целях. В настоящее время при изготовлении удостоверений используются специальные материалы и технологии, что затрудняет их подделку.

Идентификация по отпечаткам пальцев Определяемые комбинацией генов и случайными процессами во время развития плода, отпечатки пальцев на протяжении всей жизни остаются такими же, как при рождении. Отпечатки пальцев неуничтожимы. Причина их стойкости кроется в том, что рисунок линий формируется глубинными слоями эпидермиса, и единственный способ изменить чьи-либо отпечатки заключается в полном удалении кожи с подушечек и заменой её кожей с других участков тела. Но важность отпечатков пальцев для раскрытия преступлений не только в том, что они уникальны, но и в том, что они остаются на месте преступления. В отличие от системы Бертильона, нет необходимости фиксировать отпечатки пальцев всего населения, достаточно лишь сравнить обнаруженные отпечатки с отпечатками подозреваемого. Правоохранительные органы настаивают на создании реестра отпечатков пальцев, но они постоянно сталкиваются с неприятием этой идеи обществом по целому ряду причин: - чьи-либо отпечатки пальцев могут оказаться на месте преступления по вполне законной причине. Присутствие идентифицируемых отпечатков создает презумпцию виновности; - отпечатки могут быть случайно или преднамеренно перепутаны в лаборатории; - хранимые файлы с отпечатками могут быть преднамеренно изменены с целью обвинения невиновного; - экспертные заключения по анализу

отпечатков могут быть перепутаны или специально изменены. Дактилоскопирование не может гарантировать идентификацию, оно лишь обеспечивает связь конкретного пальца с записью в файле. Изменив файл, изменится идентификация. Дактилоскопия как средство строгой идентификации может быть использована репрессивными и тоталитарными режимами. Пропускная система во времена апартеида в Южной Африке и идентификационные карточки, выдаваемые палестинцам на оккупированных Израилем территориях, являются примерами таких систем идентификации. Идентификация по ДНК Идентификация по дезоксирибонуклеиновой кислоте (ДНК) основана на анализе цепочек генов и является почти безупречной. Сегодня у неё три основных применения: - установление отцовства; - определение принадлежности крови и семенной жидкости, оставленных на месте преступления; - идентификация человеческих останков. Всё чаще анализ ДНК применяется для идентификации человеческих останков. Поскольку молекула ДНК чрезвычайно стабильна, необходимый для анализа материал может быть получен из останков через годы или даже через тысячи лет после смерти человека. Несмотря на всю мощь технологий идентификации ДНК, им присущи некоторые фундаментальные проблемы: 1) ДНК не во всех случаях является уникальной: однояйцовые близнецы по определению имеют один и тот же набор хромосом. Приблизительно 0,338% населения являются однояйцовыми близнецами, т.е. три человека из тысячи. 2) При экспертизе анализируются только «мусорные участки» ДНК (ДНК двух отдельно взятых людей совпадают почти на 99%). Поскольку эти фрагменты генома не участвуют в жизнеобеспечении клеток или организма в целом, из поколения в поколение происходят их случайные изменения, или мутации. Специалисты не могут полностью исключить возможность случайного совпадения и неверной идентификации. 3) Для проведения теста требуется лабораторное оборудование и квалифицированные специалисты. Так же не следует исключать возможность того, что образцы крови или семенной жидкости с места преступления могут быть подменены при транспортировке, как случайно, так и умышленно. Компьютерная биометрия Все современные системы биометрической идентификации состоят из двух частей. Первая - это устройство, которое производит измерение какого-либо параметра человеческого тела и преобразует его в цифровую форму. Вторая - большая база данных, хранящая результаты биометрических измерений сотен, тысяч или даже миллионов людей. За последние годы было разработано множество систем биометрической идентификации. Рисунок сетчатки глаза. Сетчатка похожа по своей индивидуальности на отпечатки пальцев. В этом случае анализируется уникальный рисунок внутри глаза человека. В 1980-е годы были популярны системы, анализирующие картину, образуемую венами и артериями глаза. Однако, в отличие от отпечатков пальцев, рисунок сетчатки подвержен изменениям: у женщин

во время беременности под воздействием гормонов плода в глазу могут образовываться новые сосуды, меняющие рисунок. Эта система дискриминирует женщин, которым приходится объясняться при каждом несовпадении изображений сетчатки. Сканирование радужной оболочки. Сканирование радужной оболочки является наиболее точным и стабильным. Узор на радужке формируется до рождения и остается неизменным на протяжении всей жизни (кроме случаев травм и хирургического вмешательства). Даже однояйцовые близнецы имеют различающиеся радужные оболочки. Вероятность совпадения биометрических показателей радужки двух людей составляет один шанс из 1078 В настоящее время разработаны высокоскоростные сканеры радужной оболочки, которые могут получать изображение радужки человека, сидящего в машине, движущейся со скоростью 90 км/час. Однако сканирование радужки идентифицирует не человека, а лишь его радужную оболочку. Узнать по результатам сканирования имя человека можно только после поиска в компьютерной базе данных. Если база данных была взломана и модифицирована, сканирование радужной оболочки не даст правильной идентификации. Анализ почерка. Анализ почерка и собственноручной подписи является одной из первых биометрических систем в мире. Сегодня изображение подписи может быть оцифровано и сравнено с имеющимися образцами. Если подпись ставится на специальном электронном планшете, компьютер может также анализировать скорость перемещения пера и силу нажатия. Комбинируя эти три параметра (траекторию, скорость и силу нажатия) можно построить биометрическую модель, которую очень сложно подделать. Отпечатки ладоней и их геометрия. При идентификации по отпечатку ладони и её геометрии анализируется рисунок складок и относительная длина пальцев. Данный способ страдает нестабильностью по сравнению с анализом отпечатков пальцев, т.к. измеряемые параметры меняются со временем. Характеристики голоса. Системы голосового анализа пытаются идентифицировать говорящего путем сравнения произносимых им фраз с заранее записанными. Распознавание лица. Системы распознавания лица идентифицируют человека на основе визуального сходства. В отличие от других систем биометрической идентификации, распознавание лица носит пассивный характер: оно может осуществляться без ведома человека, позволяя производить идентификацию в лифте или при проходе через дверь. Термограмма лица. Идентификация по термограмме лица использует особенности расположения проходящих непосредственно под кожей кровеносных сосудов. Считается, что термограмма лица более надёжный способ идентификации, чем простое визуальное распознавание. Несмотря на имеющиеся достижения в использовании компьютерной биометрии, ни одна из описанных выше систем идентификации не прошла какого-либо научного обследования, как это было с идентификацией по ДНК в конце 1980-х - начале 1990-х годов. Уязвимость биометрических систем

Отпечатки пальцев, сканирование радужной оболочки глаза и анализ генных последовательностей часто рассматриваются как абсолютно безупречные способы идентификации человека. Считается, что они настолько хороши, что в ближайшей перспективе можно вполне отказаться от разного рода идентификационных карточек и паспортов. Вместо этого будет существовать единая база данных, с помощью которой гражданин может быть идентифицирован на основе уникальных признаков его собственного тела. Но остаются невыясненными ряд важных вопросов: - Кто будет контролировать доступ к банку данных? - Кто будет иметь право вносить в него изменения? - Что делать, если вдруг компьютерная система даст сбой? 7.2. Применение паролей в механизме аутентификации человека Классификация паролей. Правила создания паролей. Пароли, как правило, рассматриваются в качестве ключей для входа в систему, но они используются во всех тех случаях, когда требуется твердая уверенность в том, что соответствующие действия будут производиться только законными владельцами или пользователями программного обеспечения. Классификация паролей Пароли подразделяются на несколько основных групп: - пароли, генерируемые системой; - полуслова; - ключевые фразы; - интерактивные последовательности типа «вопрос - ответ»; - пароли, устанавливаемые пользователем. Случайные пароли и коды, устанавливаемые системой, могут быть нескольких разновидностей. Системное программное обеспечение может применить полностью случайную последовательность символов - случайную вплоть до регистров, цифр, пунктуации, длины. Полуслова частично создаются пользователем, а частично - каким-либо случайным процессом. Это значит, что если даже пользователь придумает легко угадываемый пароль, например, «секрет», компьютер дополнит его, образовав более сложный пароль типа «секрет,2rs87». Ключевые фразы трудно угадать и легко запомнить. Фразы могут быть осмысленными или не иметь смысла. В программировании постепенно намечается тенденция к переходу на более широкое применение ключевых фраз. Интерактивные последовательности «вопрос - ответ», предлагают пользователю ответить на несколько вопросов, как правило, личного плана. В компьютере хранятся ответы на множество таких вопросов. При входе пользователя в систему компьютер сравнивает полученные ответы с «правильными». Пароли, устанавливаемые пользователем. Большинство паролей относятся к типу «выбери сам». Обычно пароль содержит не менее четырех-пяти букв. Существуют также и другие меры, призванные не позволить пользователю создать неудачный пароль. Например, система может настаивать на том, чтобы пароль включал в себя строчные и заглавные буквы вперемешку с цифрами; заведомо очевидные пароли, например, «компьютер», ею отвергаются. Правила создания паролей При установке пароля существует ряд правил, которых следует придерживаться. Пароли не должны состоять из: - только цифр или одинаковых

букв; - Вашего имени, отчества или фамилии ни в каком виде (т.е. написаны в строчном, в прописном, в смешанном виде, задом наперед, два раза и т.д.); - имен Вашей (его) супруги (а) или детей; -личной информации. Сюда входят: номера телефонов, номера в пропусках и других документах, номер или марка вашего автомобиля, Ваш почтовый адрес и т.д. и т.п.; - слов, которые можно найти в словаре (любом, включая иностранные) или в каком-либо списке слов. Запрещается использовать в качестве пароля название учётной записи (идентификатора входа (login)) ни в каком виде, а так же легко угадываемые сочетания символов. Для проверки сложности паролей используют специальные контроллеры паролей. Контроллеры осуществляют попытки взлома пароля по разным методикам, например: 1. Проверка использования в качестве пароля входного имени пользователя, его инициалов и их комбинаций. 2. Проверка использования в качестве пароля слов из различных словарей: - мужские и женские имена; - названия стран и городов; - имена персонажей мультфильмов, кинофильмов, научно-фантастических произведений и т.п.; - спортивные термины (названия спортивных команд, имена спортсменов, спортивный жаргон и т.п.); - числа (цифрами и прописью); - строки букв и цифр (например, АА, ААА, АААА и т.д.); - библейские имена и названия; - биологические термины; - жаргонные слова и ругательства; - последовательности символов в порядке их расположения на клавиатуре (например, QWERTY, ASDF, ZXCVBN и т.д.); - часто употребляемые иностранные слова. 3. Проверка различных перестановок слов из п.2, включая: - замену первой буквы на прописную; - замену всех букв на прописные; - замена одной строчной буквы на прописную; - замена двух строчных букв на прописные (около 1500000 слов); - замена трех строчных букв на прописные и т.д.; - замену буквы О на цифру 0 и наоборот (цифру 1 на букву I и т.д.); - превращение слов во множественное число. Приведенные выше примеры позволяют сформулировать ряд способов снижения уязвимости паролей. Пароль должен отвечать следующим требованиям: а) быть определенной длины; б) включать в себя как прописные, так и строчные буквы; в) включать в себя одну и более цифр; г) включать в себя, как минимум, один нецифровой и неалфавитный символ. В частности пароли должны: - быть составлены так, чтобы Вы могли быстро набрать их на клавиатуре. Это осложнит возможность подглядеть пароль' - быть легко запоминаемы, чтобы не было необходимости записывать их; - длина пароля, должна составлять не менее 8 символов; - содержать небуквенные символы (т.е. цифры, знаки пунктуации, специальные символы); - при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов; - каждый пароль должен содержать как минимум две буквы (большие или малые) и хотя бы одну цифру или знак; - новый пароль должен отличаться от старого хотя бы тремя символами. При сравнении не делается

различий между большими и малыми буквами; - каждый пароль должен отличаться от входного имени, прочитанного слева направо или задом наперед, и от его циклических сдвигов. При сравнении не делается различий между большими и малыми буквами; - пользователь обязан не реже одного раза в месяц производить смену основного пароля. Важнейшими характеристиками пароля являются его длина и период смены (или период жизни). Чем больше длина пароля, тем больше усилий придется приложить нарушителю для его определения. Чем больше период жизни пароля, тем более вероятно его раскрытие. 7.3. Информационная безопасность компании Человеческий фактор в обеспечении информационной безопасности компании. Система информационной безопасности компании. Безопасное использование Интернет-ресурсов в компании. Количество компьютерных преступлений в России ежегодно растет. Это связано с повышением ценности конфиденциальной информации: она приобрела реальную стоимость, которая определяется величиной прибыли от ее использования или размером вероятного ущерба владельцу. В результате мотивы к совершению преступлений в сфере высоких технологий множатся. Как и возможности: корпоративные компьютерные сети расширяются, конфигурация их меняется, объектов вторжений в информационные системы становится все больше, а инструмен ты атак постоянно обновляются. Это лишь краткий список причин, вызывающих рост информационной преступности. Человеческий Фактор в обеспечении информационной безопасности компании Недооценивая важность защиты информации, компании делают основной упор на физическую безопасность (пропускной режим, охрану, систему видеонаблюдения и так далее). Но если десять лет назад это было оправдано, то сейчас ситуация существенно изменилась. Сейчас самая конфиденциальная информация лежит не в сейфе у директора, а на жестком диске компьютера. Чтобы заполучить необходимую информацию и нанести компании финансовый ущерб, достаточно проникнуть в ее информационную систему или вывести из строя какой-либо узел корпоративной сети. Подобные вторжения вызывают как прямой ущерб (зачастую измеряемый шести-семизначными суммами), так и косвенный: неисправность узла приводит к затратам на его восстановление (обновление или замену программного обеспечения, зарплату обслуживающего персонала). Атака на \veЬ-сервер компании и замена его содержимого на любое другое может привести к снижению доверия к фирме и, как следствие, потере части клиентуры и доходов. В зависимости от вида деятельности и целей компании можно выделить наиболее важные направления обеспечения информационной безопасности. Для одних приоритетом является предотвращение утечки информации (маркетинговых планов, перспективных разработок и так далее). Другие могут пренебречь конфиденциальностью внутренней информации и сосредоточить внимание на ее целостности. Например, для банка важно в первую

очередь обеспечить подлинность обрабатываемых платежных поручений. Для интернет-провайдера, компании, обладающей \veЬ-сервером, или оператора связи на первое место выходит задача обеспечения доступности и безотказной работы всех (или наиболее важных) информационных систем. Наиболее распространенный миф из области защиты информации, бытующий в бизнес-среде: основная опасность исходит от внешних злоумышленников, проникающих в компьютерные системы. Бесспорно, ее нельзя недооценивать, но она слишком преувеличена. Обратимся к статистике. До 80% всех ком пьютерных преступлений связано с вольными или невольными внутренними нарушениями со стороны работающих или уволенных сотрудников. Почему они совершают преступления против собственной компании? Причин множество. Самая распространенная - неудовлетворенность статусом или зарплатой. Другой нередкий случай: сотрудник при увольнении затаил обиду и хочет отомстить компании, ее руководству. Больших бед можно ждать, если злоумышленник облечен внушительными полномочиями и имеет доступ к широкому спектру информации. Громадный ущерб, например, способен нанести сотрудник отдела автоматизации, информатизации и телекоммуникаций, обладающий достаточными квалификацией и опытом: ему могут быть известны пароли ко всем используемым системам. Таких «лазутчиков» трудно обнаружить: они способны обходить защитные механизмы. Исходя из вышесказанного, прежде всего, следует убедиться в лояльности персонала компании. Принимая сотрудника на работу, необходимо всеми доступными средствами навести о нем справки. Рекомендуется: — применять специальные психологические тесты, которые помогут оценить его лояльность и психологические качества; — продумать систему материального и морального поощрения за сохранение лояльности; — оговорить в контракте с сотрудником условия сохранения конфиденциальности не только на период совместной работы, но и на определенный срок после завершения ваших взаимоотношений. Только в этом случае можно предъявлять какиелибо претензии. Однако больше всего убытков компании причиняет неграмотность и халатность персонала: В своё время неграмотное использование электронной почты привело к распространению по всему миру таких компьютерных вирусов, как Love San и I love you, убытки от которых составляют десятки, а то и сотни миллионов долларов. Половина паролей, придуманных рядовыми сотрудниками, состоят из цифр дат рождения и имени дочери или сына. Такие пароли легко вскрыть. Но даже если системный администратор назначает пароль из трудно запоминаемой комбинации букв и цифр, работники, не долго думая, на виду у всех приклеивают его на мо нитор или ставят галочку «запомнить пароль», чтобы не набирать каждый раз заново. В результате доступ к компьютеру и корпоративной сети открыт любому желающему. Большинство специалистов связывают беспечность менеджмента и персонала, во-первых, с небольшим числом получивших огласку хищений

информации «в особо крупных размерах»; во-вторых, с низким уровнем внутрикорпоративной дисциплины и обучения персонала правилам информационной безопасности. Между тем ряд отечественных компаний, например крупные холдинги, накопили большой опыт создания систем информационной безопасности. Система информационной безопасности компании Следует придерживаться комплексного подхода к решению проблемы защиты информации. Для того чтобы риск коммерческой деятельности был минимальным, надо оценить всевозможные угрозы безопасности информации с учетом двух факторов: предполагаемой вероятности возникновения угрозы и возможного ущерба от ее осуществления. На первом этапе проводится информационное обследование. Определяется, от чего в первую очередь необходимо защищаться компании. Объективность оценки угроз достигается детальным анализом функционирования компании и привлечением независимых экспертов. Строится «модель нарушителя», которая описывает его квалификацию, средства для реализации атак, обычное время их проведения и прочее. В результате вырабатываются рекомендации для устранения выявленных угроз, правильного выбора и применения средств защиты. Второй этап - приобретение, установка и настройка рекомендованных средств и механизмов, в совокупности обеспечивающих защиту системы обработки данных от посторонних лиц, системы обработки данных от пользователей, пользователей друг от друга, каждого пользователя от себя самого, системы обработки от самой себя. Что нужно делать для того, чтобы защитить информационную корпоративную сеть? - Убедиться в том, что ни один человек не имеет доступа сразу ко всем функциям системы сверху донизу. - Потребовать от каждого пользователя ввода пароля при вхождении в систему. - Предоставлять права суперпользователя как можно меньшему числу людей. - Резервную копию наиболее важных компонентов системы необходимо делать ежедневно. - Раз в неделю делать резервную копию всей системы. - Установить строгий контроль за доступом к лентам с резервными копиями. - Текущую резервную копию хранить отдельно, в надежном удаленном месте. - Регулярно копировать информацию, хранящуюся на настольных и портативных компьютерах, а также на серверах. - Менять пароли, по крайней мере, каждые три месяца. - Разместить серверы в безопасном, недоступном для посторонних месте. - Человек, обеспечивающий текущее функционирование системы, не должен отвечать за создание резервных копий. - Регулярно обновлять программное обеспечение. - Установить программное обеспечение, позволяющее обнаружить попытку несанкционированного доступа и своевременно получить соответствующее предупреждение. - Выделять на нужды безопасности не менее 3-5% бюджета информационной службы. - Персонал группы информационной безопасности должен выявлять случаи проявления сотрудниками неуверенности или недовольства (особенно это касается тех служащих, которые имеют доступ к

важным сведениям). - Уделять повышенное внимание вопросам безопасности в периоды массовых увольнений или слияния с другими фирмами. Сотрудники, раздраженные таким поворотом событий, могут предпринять действия, которые негативным образом отразятся на работе компании. - Наладить мониторинг сети. Специальные программные средства выдадут предупреждение в том случае, если пользователь проник в запрещенную для него область сети или работает в неположенное время. -Установить контроль за электронной перепиской с целью выявления подозрительных внешних контактов. - Проверять правильность и надежность создаваемых резервных копий. Возложите задачу резервного копирования еще на кого-нибудь, если сотрудник, постоянно занимающийся этими вопросами, попал под подозрение. - При подписании контракта с сотрудником оговорить все условия работы и меры наказания, принимаемые в случае различных нарушений и невыполнения предъявляемых требований. - Люди, занимающие ключевые посты в информационной службе, должны быть заинтересованы в укреплении позиций компании. С течением времени средства защиты устаревают, выходят новые версии систем обеспечения информационной безопасности, постоянно расширяется список обнаруженных атак и «брешей», меняются технология обработки информации, программные и аппаратные средства, персонал компании. Создание системы информационной безопасности - бесконечный эволюционный процесс, требующий немалых затрат. Важнейший элемент системы - корпоративная политика информационной безопасности. Основные принципы политики безопасности таковы: - никто не имеет права подходить к компьютеру сотрудника кроме самого сотрудника и системного администратора; - компьютер никогда не остается без присмотра включенным; - никто не может увидеть ни одного файла с компьютера сотрудника по сети; -применяются только те службы и протоколы, которые необходимы в данный момент. По мнению специалистов, даже выполнение элементарных требований безопасности (четкое разграничение прав доступа пользователей к системе, соблюдение правил «интернетгигиены», использование лицензионного программного обеспечения и услуг квалифицированного системного администратора) позволяет компании вдвое снизить риск компьютерного преступления. Абсолютно безопасный компьютер - это компьютер выключенный. Поэтому идеально безопасной системы не существует. Как только в ней появляется хоть один человек, она не безопасна. Люди были и есть самое слабое звено информационной безопасности. Когда речь идет об информационной безопасности, важно понимать: суть проблемы не в аудите, не в программах и даже не в конкретных людях, а в эффективно работающих процедурах, направленных на предотвращение несанкционированного доступа, поддержание системы в закрытом состоянии, в механизмах быстрого реагирования в случае нарушения целостности данных. Риск, порождаемый человеческим

фактором, можно значительно снизить политикой, инструкциями, положениями и регламентами, а также с помощью средств пропускного режима, техническими средствами. Безопасное использование Интернет-ресурсов в компании Интернет стал рабочим инструментом, без которого уже невозможно представить себе повседневную деятельность множества людей. Это и глобальная справочно-информационная система, и способ доступа к технологиям, и транспорт для передачи данных, и, наконец, оперативное и доступное средство коммуникации. Одной из особенностей Интернета является то, что на определенном этапе он развивался стихийно. Это, с одной стороны, обеспечило массовый характер его использования, а с другой - породило ряд проблем с серьезными последствиями: - поскольку Интернет является каналом во внешний мир, он стал основным источником распространения вредоносного мобильного кода (вирусов, червей, троянских программ); - глобальная сеть стала использоваться в качестве канала, через который осуществляются атаки на локальные вычислительные сети организаций, отдельные серверы и компьютеры; - Интернет стал активно применяться в качестве средства скрытого проникновения в корпоративные локальные вычислительные сети; - в настоящее время Интернет может рассматриваться как один из основных каналов утечки конфиденциальной информации. Имея доступ к Интернету со своего рабочего места и зная, что канал не контролируется, любой пользователь может беспрепятственно отправить за пределы организации любую конфиденциальную информацию; - бесконтрольный доступ к Интернету значительно снижает производительность труда в коллективе. Простота освоения, легкость поиска необходимой информации и другие полезные качества Интернета - вот причины того, что данный сервис широко применяется, в том числе и для личных целей. По данным компании IDC, около трети своего рабочего времени сотрудники различных организаций и компаний проводят в Интернете в целях, не имеющих прямого отношения к их работе; - снижение пропускной способности сети. Согласно статистике, 44% сотрудников организаций используют корпоративные ресурсы для просмотра видео, прослушивания аудиозаписей (через потоковые аудио- и видеоканалы), играют в сетевые игры, загружают файлы большого объема (например, файлы мультимедиа: графические, музыкальные файлы, фильмы и т.п.), что создает значительную нагрузку на локальные вычислительные сети. Проблему безопасного и продуктивного использования Интернет-ресурсов можно решить двумя способами. Первый - радикальное запрещение использования Интернета без необходимости. Если принят принцип «запрещено все, что явно не разрешено», пользователям разрешается доступ только к строго определенным сайтам. Второй способ - более гибкий, он позволяет пользователям действовать по принципу «разрешено все, что не запрещено». В этом случае сотрудник может свободно пользоваться ресурсами

Интернета, однако его действия находятся под контролем. Это значит, что если пользователь выполнит действия, противоречащие политике безопасности, это будет обнаружено и пресечено. В настоящее время «радикальный» способ по-прежнему находит применение. Он используется, в первую очередь, организациями, в которых циркулирует информация с грифом «секретно». К таким организациям относятся различные научноисследовательские институты, военные организации, государственные органы и специальные службы. В таких «секретных» организациях существуют инструкции и документы, которые строго регламентируют поведение пользователей, связанное с получением информации и её передачей за пределы организации. А это значительно облегчает деятельность контролирующих служб по обеспечению должного уровня защиты. Другой пример «радикального» способа - применение в компаниях так называемых Интернет-киосков, когда пользователям предоставляется доступ к Интернет-ресурсам через выделенные терминалы. Как правило, в этом случае действия пользователей строго регламентируются, а трафик, проходящий через данный терминал, контролируется специальными средствами. Большинство же коммерческих организаций и компаний предпочитают более гибкий способ регламентации общения с внешним миром. Чтобы обеспечить гибкий контроль использования Интернет-ресурсов, необходимо ввести в компании соответствующую политику использования ресурсов. Эта политика может реализовываться как «вручную», так и автоматически (при помощи специальных программ). «Ручная» реализация означает, что в организации имеется специальный штат сотрудников, которые ведут мониторинг активности пользователей. Вопросы для самоконтроля 1. Перечислите основные классы контроля доступа. 2. Перечислите методы биометрической идентификации человека. 3. Насколько методы биометрической идентификации человека могут быть точны? 4. В чём уязвимость биометрической идентификации человека? 5. Перечислите правила создания паролей. 6. Почему в обеспечении защиты информации человек является «самым слабым звеном»? 7. Что представляет собой политика информационной безопасности организации? 8. Каковы способы безопасного использования Интернет ресурсов?

АДУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аудит (контроль) состояния защиты информации — специальная проверка соответствия организации и эффективности защиты информации установлен ным требованиям и/или нормам. Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований. (Закон РФ «Об информации, информатизации и защите информации»)

Постулаты 1. Угрозы легче предупредить, чем устранять результаты их воздействия. 2. На бога надейся, а сам не плошай. 3. Дружба дружбой, а табачок врозь. Проведение независимого аудита позволяет сво евременно выявить существующие бреши и объективно оценить соответствие параметров, характеризующих режим информационной безопасности (ИБ), необходимому уровню.Для решения этих задач создаются специальные организации аудиторов в области информационной безопасности Они ставят своей целью проведение экспертизы соответствия системы информационной безопасности определенным требованиям, оценки системы управления безопасностью, повышения ква лификации специалистов в области информационной безопасности Такие организации могут быть как государственными (например, подразделения государственной технической комиссии при Президенте РФ), так и иметь статус независимых, негосударственных Аудит позволяет оценить текущую безопасность функционирования информационной системы, оценить и прогнозировать риски, управлять их влиянием на бизнес-процессы фирмы, корректно и обоснованно подойти к вопросу обеспечения безопасности ее информационных активов, стратегических планов развития, маркетинговых программ, финансовых и бухгалтерских ведомостей, содержимого корпоративных баз данных В конечном счете, грамотно проведенный аудит безопасности информационной системы позволяет добиться максимальной отдачи от средств, инвестируемых в со здание и обслуживание системы безопасности фирмы Основными направлениями деятельности в облас ти аудита безопасности информации являются 1 Аттестация объектов информатизации по требованиям безопасности информации a. аттестация автоматизированных систем, средств связи, обработки и передачи информации, b. аттестация помещений, предназначенных для ведения конфиденциальных переговоров, c. аттестация технических сре дств, установленных в выделенных помещениях 2 Контроль защищенности информации ограниченного доступа a. выявление технических каналов утечки информации и способов несанкционированного досту па к ней, b. контроль эффективности применяемых средств защиты информации 3 Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок (ПЭМИН) a. персональные ЭВМ, средства связи и обработки информации; b. локальные вычислительные системы; c. оформления результатов исследований в соответствии с требованиями Гостехкомиссии России. 4 Проектирование объектов в защищенном исполнении. a. разработка концепции информационной безопасности (первая глава учебника); b. проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении; c. проектирование помещений, предназначенных для ведения конфиденциальных переговоров. Аудит выделенных помещений Общепринятая методика аудита выделенных по мещений условно разделяет

действия по выявлению средств несанкционированного съема информации (НСИ) на три этапа: ■ подготовительный этап; ■ этап непосредственного проведения аудита; ■ заключительный этап. Подготовительный этап аудита выделенных помещений: 1 Уточнение границ и ранжирование по степени важности информации, относимой к конфиденциальной. 2 Уточнение вероятного злоумышленника, оценка его возможностей, тактики внедрения средств НСИ и их использования. 3 Разработка замысла проведения аудита выделен ных помещений: a. выработка целевой установки; b. определение масштаба и места проведения поисковых мероприятий, выбор времени проведения; c. разработка легенды, под прикрытием которой будет проводиться аудит; d. выработка замысла активации внедренных средств НСД; e. выбор вариантов действий в случае обнаружения средств НСИ. 4 Изучение планов помещений, схем технических коммуникаций, связи, организации охраны, дос тупа и других необходимых документов. 5 Предварительный осмотр объекта. 6 Разработка перечня аппаратуры, необходимой для проведения проверки помещений и объектов. 7 Разработка дополнительных мер по активации внедренных средств НСИ на время проведения поиска с различными типами аппаратуры. 8 Распределение привлекаемых сил и средств по объектам и видам работ. 9 Уточнение частных методик использования привлекаемой аппаратуры в конкретных условиях проверки. 10 Оформление плана проведения комплексной проверки помещений и объектов и утверждение его у руководителя предприятия. 11 Подготовка аппаратуры для проведения поиско вых и исследовательских работ. 12 Предварительный сбор данных и анализ радиоэлектронной обстановки в районе обследуемых объектов и помещений. 13 Подготовка документов прикрытия работ по про верке помещений в соответствии с выбранной легендой прикрытия. 14 Подготовка бланков, схем, заготовок других документов, необходимых для проведения работ на последующих этапах. Перечень специального оборудования и технических средств, рекомендуемых для проведения аудита по мещений. 1 Комплект досмотровых зеркал (ПОИСК-2, ШМЕЛЬ-2) — Визуальный осмотр оборудования, мебели, технологических коммуникаций. 2 Комплект луп, фонарей — Визуальный осмотр поверхностей и отверстий. 3 Технический эндоскоп с дистальным концом (серия ЭТ, Olimpus) — Визуальный осмотр труднодо ступных полостей и каналов. 4 Комплект отверток, ключей и радиомонтажного инструмента — Разборка и сборка коммутационных, электроустановочных и других устройств и предметов. 5 Досмотровый металлоискатель (УНИСКАН 7215, АКА 7202, Comet) — Проверка предметов и элементов интерьера на наличие металлических включений. 6 Прибор нелинейный радиолокации (NR-900EM, ОРИОН NGE-400, РОДНИК 23) — Проверка строительных конструкций и предметов на наличие радиоэлектронных компонентов. 7 Переносная рентгенотелевизионная установка (ШМЕЛЬ 90/К, ФП-1, РОНА) — Проверка элементов интерьера на наличие скрытно установленных

средств НСИ. 8 Переносный радиоприемник или магнитола — Озвучивание проверяемых помещений. 9 Многофункциональный поисковый прибор (ПИРАНЬЯ, ПСЧ-5, D-008) — Проверка проводных коммуникаций на наличие информационных сигналов. 10 Низкочастотный нелинейный детектор проводных коммуникаций (ВИЗИР, возможная замена по телефонным линиям: ТПУ-5К или SEL SP-18/T) — Проверка проводных коммуникаций на наличие нелинейности параметров линии. 11 Комплекс обнаружения радиоизлучающих средств и радиомониторинга (КРОНА-6000М, КРК, АРК-Д1, OSC-5000) —Анализ радиоэлектронной обстановки, выявление радиоизлучающих средств неглас ного съема, информации. 12 Обнаружитель скрытых видеокамер (IRIS VCF-2000, нет аналогов) — Выявление радиоизлучающих видеокамер. 13 Дозиметр поисковый (РМ-1401, НПО-3) — Обнаружение и локализация источников радиоактивного излучения. 14 Комплекс для проведения исследований на сверхнормативные побочные электромагнитные излучения (НА ВИГАТОР, ЛЕГЕНДА. ЗАРНИЦА) — Выявление информативных побочных электромагнитных излучений. 15 Комплекс для проведения акустических и виброакустических измерений СПРУТ-4А — Выявление акустических и виброакустических сигналов и наводок, исследование звуко- и виброизоляции, проверка систем зашумления. Структура плана аудита помещений: 1 выводы из оценки противника; 2 замысел проведения аудита помещений: a. целевая установка; b. перечень и краткая характеристика проверяемых помещений; c. перечень запланированных для каждого помещения поисковых работ и сопутствующих исследований; d. время проведения проверки; e. легенда, под прикрытием которой будет проводиться проверка; f. меры по активации внедренных средств НСИ; g. действия в случае обнаружения средств НСИ; 3 привлекаемые для проведения проверки силы, технические средства и их распределение по объектам и видам работ; 4 основные особенности применения технических средств, определяемые условиями проверки; 5 дополнительные меры по активизации внедренных средств НСИ; 6 перечень подготавливаемых по результатам проверки итоговых и отчетных документов и срок их представления для утверждения. Некоторые сложности могут возникнуть при орга низации предварительного сбора данных и анализа ра диоэлектронной обстановки в районе обследуемых помещений. Если служба безопасности предприятия не располагает собственным постом радиомониторинга, с руководителем предприятия должно быть согласовано место и время развертывания временного пункта ра - диоконтроля с комплектом необходимой радиоприемной и анализирующей аппаратуры. В целях конспирации желательно, чтобы это место находилось где -нибудь за территорией предприятия, но в непосредственной близости от намеченных к проверке помещений. В качестве такого пункта мы рекомендуем использовать обычный легковой автомобиль с развернутым в нем комплексом обнаружения радиоизлучающих средств и радиомониторинга. Итогом

деятельности пункта радиоконтроля на этом этапе работ должна быть карта занятости радиоэфира в условиях обычного режима работы предприятия, база данных идентифицированных радиосигна лов, а также база данных подозрительных радиоизлучений, требующих дополнительного исследования. Работы подготовительного этапа обычно завершаются разработкой документов, подтверждающих леген ду прикрытия при проведении различных видов поис ковых и исследовательских работ, а также специальных бланков и заготовок документов, ускоряющих регистрацию промежуточных результатов запланированных работ. Целесообразно заранее изготовить блан ки протоколов будущих измерений, схемы коммуникаций и планы проверяемых помещений, на которые будут наноситься отметки мест обнаружения средств НСИ и подозрительных мест, журналы регистрации заводских номеров проверенного оборудования, мест установки пломб и скрытых меток, способствующих ускорению работ при последующих специальных проверках, и т.д. Этапы непосредственного проведения аудита: 1. Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера помещений. 2. Проверка элементов строительных конструкций, мебели и других предметов интерьера помещений с использованием специальных поисковых техни ческих средств. 3. Выполнение запланированных мер по активации внедренных средств НСИ. 4. Проверка линий и оборудования проводных коммуникаций: a. линий силовой и осветительной электросети; b. линий и оборудования офисной и абонентской телефонной сети; c. линий селекторной связи; d. линий радиотрансляционной сети; e. линий пожарной и охранной сигнализации; f. линий системы часофикации и других проводных линий, в том числе, невыясненного назначения. 5. Исследование радиоэлектронной обстановки в проверяемых помещениях для выявления сигналов радиопередающих средств НСИ и их локализации. 6. Поиск средств негласного съема и передачи информации, внедренных в электронные приборы. 7. Исследование звукопроницаемости элементов конструкций, проверка трубопроводных и других технологических коммуникаций на наличие в них акустических и виброакустических сигналов из проверяемого помещения. 8. Исследование побочных электромагнитных излу чений компьютеров, оргтехники и другого оборудования для выявления в них информативных сигналов. Проверку проводных коммуникаций обычно начинают с поиска в них сигналов подслушивающих устройств или других средств съема информации. Для поиска таких сигналов используется специальная аппаратура. В случае обнаружения в линии сигнала подслуши вающего устройства осуществляют тщательный визу альный осмотр доступных участков линии и всех подключенных к линии устройств, приборов, коммутационных и электроустановочных изделий. Обычно, чтобы убедиться в отсутствии в них средств НСИ, следует провести хотя бы частичную их разборку. Тщательно осматриваются подводящие провода,

особенно в местах, где возможно несанкционированное подключение к ним каких-либо устройств или отводов. Перед осмотром элементов электросети фазы электросети, по возможности, обесточиваются. В связи с повышенной информативной ценностью для противника телефонных каналов связи проверка телефонных линий и оборудования должна проводить ся с особой тщательностью. Помимо традиционного поиска информативных сигналов мы рекомендуем проверять телефонные линии на наличие нелинейно - сти их параметров и несимметрию, которые могут быть обусловлены подключением к линии средств НСИ. Следует помнить, что индуктивные съемники информации с проводных линий не выявляются ни одним из перечисленных типов приборов. Поэтому даже применение нескольких разных по своим возможностям поисковых и анализирующих устройств все - таки не может заменить визуальный осмотр телефонных линий. Особенно детально должны быть осмотрены распределительные коробки и телефонный шкаф, поскольку там наиболее просто может быть осуществлено несанкционированное подключение к линии. Обычно параллельно с проверкой проводных ком муникаций проводится радиомониторинг помещений для выявления информативных побочных излучений оргтехники и сигналов средств НСИ, использующих радиоканал для передачи перехваченной информации. Одной из проблем современного радиомониторинга является выявление средств НСИ с нетрадицион ными видами сигналов (например, шумоподобными сигналами с фазовой манипуляцией или сигналами со сверхширокополосной частотной модуляцией) или скачкообразным изменением несущей частоты. Суще ствующие средства радиоконтроля не позволяют ав томатически идентифицировать такие излучения с сигналами средств НСИ. В этой связи для радиомониторинга помещений наиболее подходят такие автоматизированные комплексы, которые позволяют опера- тору в необходимых случаях самому проводить деталь ный анализ принимаемых сигналов. Серьезным проблемным вопросом поисковых ра бот является выявление средств НСИ, внедренных противником в ПЭВМ или другие электронные приборы. Особую сложность представляет выявление таких средств, которые были внедрены в прибор за - ранее, до появления прибора в помещении, в условиях, позволивших закамуфлировать средства съема' информации с особой тщательностью. В этой связи в важных служебных помещениях рекомендуется размещать только сертифицированные технические средства, прошедшие предварительный визуальный осмотр и специальную проверку. Напомним, что такую процедуру должны проходить не только новые электронные приборы, но и любые новые предметы и подарки, включая книги, видеокассеты, пепельницы и т.п. В случае подозрения на возможность внедрения противником средств НСИ в ПЭВМ или другие электронные приборы следует провести детальное обследование этих приборов. Прежде всего проверяемый прибор необходимо разместить отдельно от

другие подключить его к электросети и попытаться с помощью индикатора поля зафиксировать факт наличии или отсутствия радиоизлучения внедренного средств съема информации. Поиск излучения целесообразно повторить после приведения прибора в рабочее состояние (включения прибора). Затем с помощью прибор ПСЧ-5 или ему подобного следует убедиться в наличии или отсутствии сигналов, возможно передаваемы: внедренным средством по проводам электрической сети или, если они есть, другим подключенным к при бору проводным линиям. Следующая стадия обследования — разборка при бора и тщательный визуальный осмотр его содержимого. В процессе осмотра обращают внимание на наличие в приборе нестандартных или дополнительных плат, радиоэлементов, следов не фабрично го монтажа. С особой тщательностью, с помощью лупы осматривают крупно габаритные детали: микросхемы, электролитические конденсаторы, мощные транзисторы, коммутационны элементы. Существенную помощь при этом могут оказать ранее сделанные фотографии расположения элементов монтажа на платах аналогичного прибора. В отчетных документах по проведению специальной проверки помещений обычно требуется оценит возможность утечки информации по различным техническим каналам. Для этого проводятся специальные исследования, включающие исследование ПЭМИ компьютеров и других средств оргтехники, наводок возникающих за счет ПЭМИ и взаимного влияния электромагнитных полей проводных линий, информативных сигналов в цепях заземления, виброакустических сигналов в элементах конструкции помещений и другие. Заключительный этап работ по комплексной специальной проверке помещений заключается в обработке результатов исследований, проведении необходимых инженерных расчетов, разработке и представлении руководству отчетных и итоговых документов Итоговым документом, завершающим работы по обследованию помещений на наличие средств НСИ является акт проведения комплексной специальной проверки помещений. Акт подписывается руководителем и членами поисковой бригады, согласовывается с руководителем организации, проводившей поисковые работы, и утверждается руководителем предприятия. Этот документ обычно включает: ■ время проведения специальной проверки; ■ состав поисковой бригады; ■ перечень проверенных помещений и объектов; ■ перечень и объем основных поисковых работ и сопутствующих исследований; ■ перечень использовавшейся поисковой и исследовательской аппаратуры; ■ результаты специальной проверки: ■ место обнаружения средства НСИ, их состоя ние и краткие характеристики; ■ принятые по отношению к обнаруженным средствам меры; ■ выводы из оценки существующей степени защищенности помещений и объектов от утечки конфиденциальной информации по различным каналам; ■ рекомендации по повышению защищенности помещений и объектов и предотвращению съема информации по выявленным техническим каналам ее утечки. Заключительный этап комплексной специальной

проверки помещений: 1. Обработка результатов исследования, оформление протоколов измерений, регистрационных журналов, проведение необходимых инженерных расчетов. 2. Определение технических характеристик, потребительских свойств изъятых средств НСИ, ориентировочного времени и способов их внедрения. 3. Составление описания проведенных работ и исследований с приложением необходимых схем и планов помещений. 4. Разработка рекомендаций по повышению защищенности проверенных помещений и объектов: ♣ составление перечня и схем выявленных технических каналов утечки информации по каждому помещению и объекту; ♣ оценка степени существующей защиты каждого помещения и объекта от негласного съема информации по выявленным каналам ее утечки; ♣ разработка дополнительных мер и способов щиты по каждому каналу и помещению (организационных, в том числе: режимных, инженерно-технических). 5. Составление сводного перечня технических сред и систем, рекомендуемых к установке для защиты информации от утечки по техническим каналам. 6. Разработка предложений по способам использования рекомендуемых технических средств и систем и объединению их в единую комплексную систему защиты информации. 7. Составление акта проведения комплексной специальной проверки помещений. 8. Представление итоговых и отчетных документов руководителю предприятия для утверждения. К числу отчетных документов относится описание проведенных работ и исследований. В состав этого документа в качестве приложений входят протоке измерений, необходимые инженерно-технические выкладки, планы помещений с указанием места разрушения аппаратуры, обнаруженных средств НСИ и технических каналов утечки информации. В этих документах указывается: аппаратура, использованная для проведения измерений, ее заводские номера и даты последних проверок, методика проведения измерений уровни обнаруженных сигналов, их частоты и другие параметры. Для руководства предприятия, заказавшего поведение комплексной специальной проверки помещений, наибольший интерес, помимо результатов поиска средств НСИ, представляют рекомендации по повышению защищенности проверенных помещений предотвращению съема информации по выявленным техническим каналам ее утечки. В зависимости объема и степени детализации эти рекомендации могут составлять отдельный отчетный документ. Зачастую руководство предприятия ожидает от специалистов строгих количественных оценок степени защиты каждого помещения и объекта от негласного съема информации по всем выявленным каналам ее утечки. На практике такие оценки удается получить далеко не всегда, ибо они требуют проведения дополнительных исследований и расчетов, как прави ло, выходящих за рамки специальной проверки помещений. Обычно приходится ограничиваться указанием зон энергетической доступности источников информативных сигналов, ранжированием выявленных каналов утечки информации

по степени угроз, экспертными оценками вероятности съема информации различными видами специальных технических средств и другими аналогичными показателями. При разработке рекомендаций по перекрытию каналов утечки информации следует руководствовать ся соображениями здравого смысла. Меры защиты должны быть адекватны степени угроз, в противном случае все финансовые ресурсы предприятия могут целиком уйти на создание системы защиты информации. Опытный специалист, владеющий основами системного мышления, всегда может найти такую комбинацию организационных, инженерных, технических мер и способов защиты, которая будет близка к опти - мальной по универсальному критерию «эффектив ность стоимость». Простой набор мер и средств защиты информации нейтрализует лишь отдельные угрозы ее безопасности, оставляя бреши в обороне. Только постоянно развивающаяся система информационной безопасности может сдержать натиск непрерывно совершенствующихся средств и методов негласного съема информации. Выводы 1. Аудит информационной безопасности фирмы — это мощное средство оценки состояния защиты информации. 2. Аудит может проводиться как собственными си лами СБ фирмы, так силами специальных лицензированных аудиторских фирм. 3. Регулярность, периодичность и масштабность аудита определяются реальной обстановкой общей безопасности предприятия.