### Введение в информационную безопасность

Словосочетание "**информационная безопасность"** в разных контекстах может иметь различный смысл. **Под информационной безопасностью** мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

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

Ежегодно 30 ноября отмечается Международный день защиты информации. Его целью является напоминание пользователям о необходимости защиты компьютеров и всей хранимой в них информации. Праздник был учрежден 30 ноября 1988 года. 2 ноября 1988 года была зафиксирована первая массовая эпидемия "червя" Морриса, получившего название по имени своего создателя - Роберта Морриса, аспиранта факультета Вычислительной техники Корнелльского университета.

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

Возвращаясь к вопросам терминологии, стоит отметить, что термин "**компьютерная безопасность**" (как эквивалент или заменитель ИБ) представляется слишком узким. Компьютеры – только одна из составляющих информационных систем. Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций, обслуживающий персонал.

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

**Доктрина информационной безопасности РФ**

Доктрина информационной безопасности Российской Федерации была утверждена 5 декабря 2016 года указом президента Российской Федерации №646. Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. В ней под **информационной сферой** понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

С точки зрения Доктрины информационной безопасности под информационной безопасностью понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

**В Доктрине выделяются следующие национальные интересы Российской Федерации в информационной сфере**:

1. обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий;
2. обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;
3. развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;
4. доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;
5. содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

В Доктрине выделяются с**тратегические цели обеспечения информационной безопасности:**

1. Стратегической целью обеспечения информационной безопасности **в области обороны** страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.
2. Стратегическими целями обеспечения информационной безопасности **в области государственной и общественной безопасности** являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры.
3. Стратегическими целями обеспечения информационной безопасности **в экономической сфере** являются сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности.
4. Стратегической целью обеспечения информационной безопасности **B области науки, технологий и образования** является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности.
5. Стратегической целью обеспечения информационной безопасности **B области стратегической стабильности и равноправного стратегического партнерства** является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

### Угрозы информационной безопасности и их классификация

**Угроза** - это потенциальная возможность определенным образом нарушить информационную безопасность. Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы**.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется **окном опасности**, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС. Если речь идет об ошибках в ПО, то окно опасности "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

* должно стать известно о средствах использования пробела в защите;
* должны быть выпущены соответствующие заплаты;
* заплаты должны быть установлены в защищаемой ИС.

Новые уязвимые места и средства их использования появляются постоянно и это значит, что почти всегда существуют окна опасности и отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат - оперативно.

Угрозы можно классифицировать по нескольким критериям:

* по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
* по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
* по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
* по расположению источника угроз (внутри/вне рассматриваемой ИС).

### Основные угрозы доступности

**Доступность** – это возможность за приемлемое время получить требуемую информационную услугу.

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это наносит ущерб всем субъектам информационных отношений. Поэтому доступность выделяется как важнейший элемент информационной безопасности. Особенно ярко ведущая роль доступности проявляется в различных системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Самыми частыми являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). Самый радикальный способ борьбы с непреднамеренными ошибками - максимальная автоматизация и строгий контроль.

Другие угрозы доступности можно классифицировать по компонентам ИС, на которые нацелены угрозы:

* отказ пользователей;
* внутренний отказ информационной системы;
* отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

* нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей, фактическими возможностями и техническими характеристиками);
* невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
* невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

* отступление (случайное или умышленное) от установленных правил эксплуатации;
* выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
* ошибки при конфигурировании системы;
* отказы программного и аппаратного обеспечения;
* разрушение данных;
* разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

* нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
* разрушение или повреждение помещений;
* невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые "обиженные" сотрудники - нынешние и бывшие, так как потенциально могут нанести вред организации-"обидчику", например:

* испортить оборудование;
* встроить логическую бомбу, которая со временем разрушит программы и/или данные;
* удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия,- пожары, наводнения, землетрясения, ураганы.

Угрозы доступности могут выглядеть грубо - как повреждение или даже разрушение оборудования. Такое повреждение может вызываться естественными причинами (чаще всего - грозами), опасны протечки водопровода и отопительной системы, поломки кондиционеров в сильную жару. Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранятся небрежно.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться **агрессивное потребление ресурсов** (обычно - полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника угрозы такое потребление подразделяется на локальное и удаленное. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю или, например, количество подключившихся пользователей ограничено ресурсами системы. Примером удаленного потребления ресурсов являются DoS-атаки – атаки на отказ в обслуживании.

### Основные угрозы целостности

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

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений. Соответствующие действия в сетевой среде называются активным прослушиванием. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

* ввести неверные данные;
* изменить данные.

Например, заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль. Последнее возможно даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов информационной безопасности: если нарушена конфиденциальность, может пострадать целостность. Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить "неотказуемость", компьютерные данные не могут рассматриваться в качестве доказательства.

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

Потенциально уязвимы с точки зрения нарушения **целостности** не только **данные**, но и **программы**. Внедрение вредоносного ПО - пример подобного нарушения.

**Основные угрозы конфиденциальности**

**Конфиденциальность** – это защита от несанкционированного доступа к информации.

Конфиденциальную информацию можно разделить **на предметную и служебную**. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе. Невозможно помнить много разных паролей; рекомендации по их регулярной смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым и угадываемым паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита. В этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п).

Перехват данных - очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их не составляет труда.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных.

Опасной нетехнической угрозой конфиденциальности являются такие методы как маскарад - выполнение действий под видом лица, обладающего полномочиями для доступа к данным.

К угрозам, от которых трудно защититься, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример - нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается на серьезные трудности.

### Объектно-ориентированный подход к информационной безопасности

Объектно-ориентированный подход является основой современной технологии программирования, испытанным методом борьбы со сложностью систем. Представляется естественным и необходимым, стремление распространить этот подход и на системы информационной безопасности. Сложны не только аппаратно-программные системы, которые необходимо защищать, но и сами средства безопасности.

Сложная система информационной безопасности на верхнем уровне должна состоять из небольшого числа относительно независимых компонентов. Относительная независимость понимается как минимизация числа связей между компонентами. Затем декомпозиции подвергаются выделенные на верхнем уровне компоненты, и так далее вниз до заданного уровня детализации. В результате система оказывается представленной в виде иерархии с несколькими уровнями абстракции. Объектно-ориентированный подход использует объектную декомпозицию, то есть поведение системы описывается в терминах взаимодействия объектов.

Весьма распространенной конкретизацией объектно-ориентированного подхода являются компонентные объектные среды. Здесь используется два важных понятия: компонент и контейнер. Компонент можно определить как многократно используемый объект, допускающий обработку в графическом инструментальном окружении и сохранение в долговременной памяти. Контейнеры могут включать в себя множество компонентов и выступать в роли компонентов других контейнеров.

Компонентные объектные среды обладают всеми достоинствами, присущими объектно-ориентированному подходу:

* инкапсуляция объектных компонентов скрывает сложность реализации, делая видимым только предоставляемый вовне интерфейс;
* наследование позволяет развивать созданные ранее компоненты, не нарушая целостность объектной оболочки;
* полиморфизм дает возможность группировать объекты, характеристики которых с некоторой точки зрения можно считать сходными.

Применяя объектно-ориентированный подход к вопросам информационной безопасности, можно ввести **понятие грани**. Фактически три грани уже были введены: это доступность, целостность и конфиденциальность. Их можно рассматривать относительно независимо, и считается, что если все они обеспечены, то обеспечена и ИБ в целом (то есть субъектам информационных отношений не будет нанесен неприемлемый ущерб). Таким образом **цель** структурирована. Средства достижения цели можно структурировать по следующим граням:

* законодательные меры обеспечения информационной безопасности;
* административные меры (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
* процедурные меры (меры безопасности, ориентированные на людей);
* программно-технические меры.

Законы и нормативные акты ориентированы на всех субъектов информационных отношений независимо от их организационной принадлежности (это могут быть как юридические, так и физические лица) в пределах страны (международные конвенции имеют даже более широкую область действия).

Административные меры ориентированы на всех субъектов в пределах организации, процедурные меры – на отдельных людей (или небольшие категории субъектов), программно-технические меры – на оборудование и программное обеспечение.

При такой трактовке в переходе с уровня на уровень осуществляется наследование (каждый следующий уровень не отменяет, а дополняет предыдущий), полиморфизм (субъекты выступают сразу в нескольких ролях - например, как инициаторы административных мер и как обычные пользователи, обязанные этим мерам подчиняться) и инкапсуляция (для фиксированной грани в одной совокупности (например, доступности) грани в другой совокупности должны пробегать все множество возможных значений от законодательных, административных, процедурных до программно-технических мер).

**Законодательный уровень**

**обеспечения информационной безопасности**

**Законодательный уровень** является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

На законодательном уровне можно выделить две группы мер:

* **меры ограничительной направленности** - меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности;
* **меры созидательной направленности** - направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

На практике обе группы мер важны в равной степени, но хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года. В соответствии **со статьей 24 Конституции**, 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.

Право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений.

**Статья 23 Конституции** гарантирует право на личную и семейную тайну, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, **статья 29** - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

**Глава 28 Уголовного кодекса Российской Федерации**

Весьма продвинутым в плане информационной безопасности является **Уголовный кодекс** Российской Федерации. **Глава 28** - "Преступления в сфере компьютерной информации" - содержит три статьи:

* статья 272. Неправомерный доступ к компьютерной информации;
* статья 273. Создание, использование и распространение вредоносных компьютерных программ;
* статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

# Статья 272. Неправомерный доступ к компьютерной информации

1. [Неправомерный доступ](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/) к охраняемой законом компьютерной информации, если это деяние повлекло [уничтожение](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/), [блокирование](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/), [модификацию](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/) либо [копирование](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/) компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные [частями первой](https://www.consultant.ru/document/cons_doc_LAW_453968/5c337673c261a026c476d578035ce68a0ae86da0/#dst970) или [второй](https://www.consultant.ru/document/cons_doc_LAW_453968/5c337673c261a026c476d578035ce68a0ae86da0/#dst972) настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего [служебного положения](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100033), -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные [частями первой](https://www.consultant.ru/document/cons_doc_LAW_453968/5c337673c261a026c476d578035ce68a0ae86da0/#dst970), [второй](https://www.consultant.ru/document/cons_doc_LAW_453968/5c337673c261a026c476d578035ce68a0ae86da0/#dst972) или [третьей](https://www.consultant.ru/document/cons_doc_LAW_453968/5c337673c261a026c476d578035ce68a0ae86da0/#dst974) настоящей статьи, если они повлекли [тяжкие последствия](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100036) или создали [угрозу](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100037) их наступления, -

наказываются лишением свободы на срок до семи лет.

Примечания.

1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

# Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. [Создание](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [распространение](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/) или [использование](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/) компьютерных [программ](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100036) либо [иной](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100023) [компьютерной информации](https://www.consultant.ru/document/cons_doc_LAW_453968/5c337673c261a026c476d578035ce68a0ae86da0/#dst978), заведомо предназначенных для несанкционированного [уничтожения](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [блокирования](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [модификации](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [копирования](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100028) компьютерной информации или [нейтрализации](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100016) средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные [частью первой](https://www.consultant.ru/document/cons_doc_LAW_453968/a4d58c1af8677d94b4fc8987c71b131f10476a76/#dst981) настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие [крупный ущерб](https://www.consultant.ru/document/cons_doc_LAW_453968/5c337673c261a026c476d578035ce68a0ae86da0/#dst979) или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные [частями первой](https://www.consultant.ru/document/cons_doc_LAW_453968/a4d58c1af8677d94b4fc8987c71b131f10476a76/#dst981) или [второй](https://www.consultant.ru/document/cons_doc_LAW_453968/a4d58c1af8677d94b4fc8987c71b131f10476a76/#dst983) настоящей статьи, если они повлекли [тяжкие последствия](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100036) или создали [угрозу](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100037) их наступления, -

наказываются лишением свободы на срок до семи лет

# Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение [правил](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100033) эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее [уничтожение](https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/), [блокирование](https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/), [модификацию](https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/) либо [копирование](https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/) [компьютерной информации](https://www.consultant.ru/document/cons_doc_LAW_453968/5c337673c261a026c476d578035ce68a0ae86da0/#dst978), причинившее [крупный ущерб](https://www.consultant.ru/document/cons_doc_LAW_453968/5c337673c261a026c476d578035ce68a0ae86da0/#dst979), -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное [частью первой](https://www.consultant.ru/document/cons_doc_LAW_453968/b5a4306016ca24a588367791e004fe4b14b0b6c9/#dst988) настоящей статьи, если оно повлекло [тяжкие последствия](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100036) или создало [угрозу](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100037) их наступления, -

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

**УК РФ Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации**

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на [критическую информационную инфраструктуру](https://www.consultant.ru/document/cons_doc_LAW_451723/c5051782233acca771e9adb35b47d3fb82c9ff1c/#dst100017) Российской Федерации, в том числе для [уничтожения](https://www.consultant.ru/document/cons_doc_LAW_10699/34672bc8c82c4b6f4b7c8cd4e77a9f414fed6cb1/), [блокирования](https://www.consultant.ru/document/cons_doc_LAW_10699/34672bc8c82c4b6f4b7c8cd4e77a9f414fed6cb1/), [модификации](https://www.consultant.ru/document/cons_doc_LAW_10699/34672bc8c82c4b6f4b7c8cd4e77a9f414fed6cb1/), [копирования](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100028) информации, содержащейся в ней, или [нейтрализации](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100016) средств защиты указанной информации.

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации.

**УК РФ Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования**

1. Нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования либо несоблюдение технических условий их установки или требований к сетям связи при использовании указанных технических средств, совершенные должностным лицом или индивидуальным предпринимателем, подвергнутыми административному наказанию за деяние, предусмотренное [частью 2 статьи 13.42](https://www.consultant.ru/document/cons_doc_LAW_435005/01db86fb46c88f00ff06171e17bb7d66fcf09a53/#dst9367) Кодекса Российской Федерации об административных правонарушениях.

2. Нарушение требований к пропуску трафика через технические средства противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования, совершенное должностным лицом или индивидуальным предпринимателем, подвергнутыми административному наказанию за деяние, предусмотренное [частью 2 статьи 13.42.1](https://www.consultant.ru/document/cons_doc_LAW_435005/ca09ff80b99766474e3ee172d0d144afc1c8581c/#dst10019) Кодекса Российской Федерации об административных правонарушениях.

**Закон «О государственной тайне» от 21 июля 1993 года N 5486-1.**

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в **Законе «О государственной тайне»**. В нем **государственная тайна** определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение **средств защиты информации**. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Закон устанавливает **три степени секретности сведений**, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "особой важности", "совершенно секретно" и "секретно".

К органам защиты государственной тайны относятся межведомственная комиссия по защите государственной тайны, другие уполномоченные органы федеральной исполнительной власти.

**Статья 283 УК РФ. Разглашение государственной тайны.**

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены -

наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок **до 4 лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, -

наказывается лишением свободы на срок **от 3 до 7 лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

**Статья 284 УК РФ. Утрата документов, содержащих государственную тайну.**

**Закон «О коммерческой тайне» №98-ФЗ от 2004 года.**

**Коммерческая тайна** - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

**Информация, составляющая коммерческую тайну** (секрет производства) - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.

В **статье 10 «Охрана конфиденциальности информации»** говорится, что меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных выше.

В **статье 11** говорится, что в целях охраны конфиденциальности информации работодатель обязан:

1) ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой является работодатель и его контрагенты;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение.

**Статья 183 УК РФ. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну**

1. Собирание сведений, … , путем похищения документов, обмана, шантажа, принуждения, подкупа или угроз, а равно иным незаконным способом-

штраф **до 500 000** рублей, лишение свободы на срок **до 2 лет**.

2. Незаконные разглашение или использование сведений, … , без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, -

штраф **до 1 000 000** рублей, лишение свободы на срок **до 2 лет**.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

штраф **до 1 500 000** рублей, лишение свободы на срок **до 5 лет**.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, -

лишение свободы на срок **до 7 лет**.

**Закон “О персональных данных” №152-ФЗ от 2006 года**

**Целью закона** является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну (статья 2).

В законе дается определение **персональных данных** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (статья 3).

**В статье 5** говорится о принципах обработки персональных данных. Это:

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

**В статье 6** говорится об условиях обработки персональных данных:

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с [законодательством](http://garant.tn.ru:81/document?id=12056199&sub=3) Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

4) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с [Федеральным законом](http://garant.tn.ru:81/document?id=12077515&sub=0) от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в [статье 15](#sub_15) настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно [статьями 10](#sub_10) и [11](#sub_11) настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

**В статье 8** говорится об общедоступных источниках персональных данных:

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

2. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

**В статье 9** говорится, что обработка ПД осуществляется с согласия субъекта ПД, который также может отозвать свое согласие на обработку своих ПД при определенных условиях. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на оператора. Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе либо аналогичные данные представителя субъекта ПД;

2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5)наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

6) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

7) срок, в течение которого действует согласие, а также порядок его отзыва;

8) собственноручную подпись субъекта персональных данных.

**В статье 10** говорится, что обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается. Исключение составляют угрозы здоровью субъекту персональных данных, обработка персональных данных в медико-профилактических целях и в правоохранительных целях и др. при соблюдении определенных условий.

**В статье 14** говорится о праве субъекта персональных данных на доступ к своим персональным данным.

**В статье 15** говорится о правах субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

**В статье 19** говорится о мерах по обеспечению безопасности персональных данных при их обработке. В частности, что оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

**В статье 21** говорится, чтовслучае достижения цели обработки персональных данных или отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в течении трех рабочих дней, если иное не предусмотрено соглашением между оператором и субъектом персональных данных или федеральными законами. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

**В статье 22** говорится об уведомлении об обработке персональных данных, что оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

7) включенных в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) в случае, если оператор осуществляет деятельность по обработке персональных данных исключительно без использования средств автоматизации;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

**Закон "Об информации, информационных технологиях и о защите информации**" **от 27 июля 2006 года N 149-ФЗ**.

Закон на первое место ставит сохранение конфиденциальности информации.

Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

В **статье 3** закона говорится о принципах правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации. Это:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

5) достоверность информации и своевременность ее предоставления;

6) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

В **статье 5** информация, в зависимости от категории доступа к ней, подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

В **статье 9** по вопросам ограничения доступа к информации говорится:

1. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

2. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

3. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

4. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

В **статье 16** говорится о защите информации:

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа,

3) реализацию права на доступ к информации.

Закон вводит понятие информационной системы и их подразделение на государственные, муниципальные и иные.

**Закон "О лицензировании отдельных видов деятельности"**

Закон номер 128-ФЗ принят Государственной Думой 13 июля 2001 года и действует с 8 августа 2001 года.

**Статья 17** Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. С точки зрения предмета ИБ интересны следующие виды:

* распространение шифровальных (криптографических) средств;
* техническое обслуживание шифровальных (криптографических) средств;
* предоставление услуг в области шифрования информации;
* разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
* выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* разработка и (или) производство средств защиты конфиденциальной информации;
* техническая защита конфиденциальной информации;
* разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;
* изготовление экземпляров аудиовизуальных произведений, программ для ЭВМ, баз данных и фонограмм на любых видах носителей (за исключением случаев, если указанная деятельность самостоятельно осуществляется лицами, обладающими правами на использование указанных объектов авторских и смежных прав в силу федерального закона или договора).

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

* деятельность, связанная с защитой государственной тайны;
* деятельность в области связи;
* образовательная деятельность.

# Срок действия лицензии не может быть менее 5 лет.

# Основные лицензирующие и контролирующие органы и их функции

# Основными лицензирующими и контролирующими органами в области защиты информации являются:

# Федеральная служба безопасности (ФСБ);

# Федеральная служба по техническому и экспортному контролю – ФСТЭК(ранее Гостехкомиссия при Президенте РФ);

# Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

# ФСБ ведает всем, что связано с криптографией, ФСТЭК лицензирует деятельность по защите конфиденциальной информации (Положение о сертификации средств защиты информации по требованиям безопасности информации). Все эти вопросы регламентированы соответствующими указами Президента и постановлениями Правительства РФ.

# В соответствии со статьей 23 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» Уполномоченным органом по защите прав субъектов Российской Федерации является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи. В настоящее время Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор – www.rsoc.ru), а именно, одно из ее управлений – Управление по защите прав субъектов персональных данных.

**ФСТЭК** России - это федеральный орган исполнительной власти, обладающий следующими полномочиями:

* обеспечение безопасности информации в ключевых системах информационной и телекоммуникационной инфраструктуры;
* организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации и руководство ею;
* обеспечение технической защиты информации некриптографическими методами;
* создание средств защиты информации, содержащей сведения, составляющие государственную тайну;
* организация и проведение лицензирования деятельности по осуществлению мероприятий и/или оказанию услуг в области защиты государственной тайны (в части, касающейся противодействия техническим разведкам и/или технической защиты информации);
* разработка и/или производство средств защиты конфиденциальной информации, а также лицензирование иных видов деятельности в соответствии с законодательством Российской Федерации;
* организация разработки программ стандартизации, технических регламентов и национальных стандартов в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, обеспечения безопасности применяемых информационных технологий, а также в области противодействия техническим разведкам и технической защиты информации.
* осуществление экспортного контроля.

В подчинении ФСТЭК России находятся территориальные органы (управления ФСТЭК России по федеральным округам), Государственный научно-исследовательский испытательный институт проблем технической защиты информации и другие подведомственные организации.

**Гражданский кодекс Российской Федерации**

За обеспечение защиты авторских и смежных прав отвечает 4 глава гражданского кодекса РФ, вступившая в действие с 01.01.2008 года.

**Статья 1225.** **Охраняемые результаты интеллектуальной деятельности и средства** **индивидуализации**

1. Результатами интеллектуальной деятельности и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальной собственностью), являются:

2) программы для ЭВМ;

3) базы данных.

**Статья 1236. Виды лицензионных договоров**

1. Лицензионный договор может предусматривать:

1) предоставление лицензиату права использования результата интеллектуальной деятельности или средства индивидуализации с сохранением за лицензиаром права выдачи лицензий другим лицам (**простая (неисключительная) лицензия**);

2) предоставление лицензиату права использования результата интеллектуальной деятельности или средства индивидуализации без сохранения за лицензиаром права выдачи лицензий другим лицам (**исключительная лицензия**).

**Статья 1259. Объекты авторских прав**

К объектам авторских прав также относятся программы для ЭВМ, которые охраняются как литературные произведения.

**Статья 1261.** **Программы для ЭВМ**

Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы. **Программой для ЭВМ** является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

**Статья 1273.** **Свободное воспроизведение произведения в личных целях**

Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение гражданином исключительно в личных целях правомерно обнародованного произведения, за исключением:

3) воспроизведения программ для ЭВМ, кроме случаев, предусмотренных [статьей 1280](#sub_41280) настоящего Кодекса;

**Статья 1280.** **Свободное воспроизведение программ для ЭВМ и баз данных. Декомпилирование программ для ЭВМ**

1. Лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных (пользователь), вправе без разрешения автора или иного правообладателя и без выплаты дополнительного вознаграждения:

1) внести в программу для ЭВМ или базу данных изменения исключительно в целях их функционирования на технических средствах пользователя и осуществлять действия, необходимые для функционирования таких программы или базы данных в соответствии с их назначением, в том числе запись и хранение в памяти ЭВМ (одной ЭВМ или одного пользователя сети), а также осуществить исправление явных ошибок, если иное не предусмотрено договором с правообладателем;

2) изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных не может быть использована в иных целях, чем цели, указанные в [подпункте 1](#sub_4128011) настоящего пункта, и должна быть уничтожена, если владение экземпляром таких программы или базы данных перестало быть правомерным.

2. Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения изучать, исследовать или испытывать функционирование такой программы в целях определения идей и принципов, лежащих в основе любого элемента программы для ЭВМ, путем осуществления действий, предусмотренных [подпунктом 1 пункта 1](#sub_4128011) настоящей статьи.

3. Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, при соблюдении следующих условий:

1) информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;

2) указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;

3) информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ.

4. Применение положений, предусмотренных настоящей статьей, не должно наносить неоправданный ущерб нормальному использованию программы для ЭВМ или базы данных и не должно ущемлять необоснованным образом законные интересы автора или иного правообладателя.

**Статья 1286.** **Лицензионный договор о предоставлении права использования произведения**

3. Заключение лицензионных договоров о предоставлении права использования программы для ЭВМ или базы данных допускается путем заключения каждым пользователем с соответствующим правообладателем договора присоединения, условия которого изложены на приобретаемом экземпляре таких программы или базы данных либо на упаковке этого экземпляра. Начало использования таких программы или базы данных пользователем, как оно определяется этими условиями, означает его согласие на заключение договора.

**Статья 1301.** **Ответственность за нарушение исключительного права на произведение**

В случаях нарушения исключительного права на произведение автор или иной правообладатель наряду с использованием других применимых способов защиты и мер ответственности, установленных настоящим Кодексом ([статьи 1250](#sub_41250), [1252](#sub_41252) и [1253](#sub_41253)), вправе в соответствии с [пунктом 3 статьи 1252](#sub_412523) настоящего Кодекса требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации:

в размере от 10 000 рублей до 5 000 000 рублей, определяемом по усмотрению суда;

в двукратном размере стоимости экземпляров произведения или в двукратном размере стоимости права использования произведения, определяемой исходя из цены, которая при сравнимых обстоятельствах обычно взимается за правомерное использование произведения.

Кроме этого в 4 главе ГК рассматриваются права изготовителя базы данных.

В Кодексе об административных правонарушениях (КоАП РФ) в статье 7.12 **«Нарушение авторских и смежных прав, изобретательских и патентных прав»** также предусмотрена ответственность:

наложение административного штрафа на граждан в размере от 1 500 до 2 000 рублей с конфискацией; на должностных лиц - от 10 000 до 20 000 рублей с конфискацией; на юридических лиц - от 30 000 до 40 000 рублей с конфискацией контрафактных экземпляров произведений и фонограмм, а также материалов и оборудования, используемых для их воспроизведения, и иных орудий совершения административного правонарушения.

**Статья 146 УК РФ. Нарушение авторских и смежных прав**

1. Присвоение авторства (плагиат), если это деяние причинило крупный ущерб автору или иному правообладателю, -

штраф **до 200 000** рублей, арест на срок до 6 месяцев.

2. Незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере, -

штрафом **до** **200 000** рублей, лишение свободы на срок **до 2 лет**.

3. Деяния, если они совершены группой лиц, в особо крупном размере или лицом с использованием своего служебного положения, -

лишение свободы на срок **до 6 лет** со штрафом в размере **до** **500 000** рублей.

Деяния признаются совершенными в крупном размере, если стоимость экземпляров произведений или фонограмм либо стоимость прав на использование объектов авторского права и смежных прав превышают **500 000** рублей, а в особо крупном размере – **2 000 000** рублей.

**Кодекс об административных правонарушениях Российской Федерации**

**Статья 13.12.** **Нарушение правил защиты информации**

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации - штраф

на граждан в размере **от 1 000 до 1 500** рублей;

на должностных лиц **от 1 500 до 2 500** рублей;

на юридических лиц **от 15 000 до 25 000** рублей.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - штраф с конфискацией

на граждан в размере **от 1 500 до 2 500** рублей;

на должностных лиц **от 2 500 до 3 000** рублей;

на юридических лиц **от 20 000 до 25 000** рублей.

3. Нарушение [условий](https://www.consultant.ru/document/cons_doc_LAW_34661/721c5c0cd868c2438ea66f09091f3a352bd56365/), предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну.

**Статья 13.13.** **Незаконная деятельность в области защиты информации**

1. Занятие видами деятельности в области защиты информации без лицензии – штраф с конфискацией или без

на граждан **от 500 до 1 000** рублей;

на должностных лиц **от 2 000 до 3 000** рублей;

на юридических лиц **от 10 000 до 20 000** рублей.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, без лицензии – штраф с конфискацией или без

на должностных лиц **от 4 000 до 5 000** рублей;

на юридических лиц **от 30 000 до 40 000** рублей.

**Статья 13.11.** **Нарушение законодательства Российской Федерации в области персональных данных**

1. Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных -

влечет наложение административного штрафа

на граждан в размере **от 10 000 до 15 000 рублей**;

на должностных лиц - **от 50 000 до 100 000 рублей**;

на юридических лиц - **от 150 000 до 300 000 рублей**.

2. Обработка персональных данных без согласия в письменной, либо обработка

персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной -

влечет наложение административного штрафа

на граждан в размере от 10 000 до 15 000 рублей;

на должностных лиц - от 100 000 до 300 000 рублей;

на юридических лиц - от 300 000 до 700 000 рублей.

**Статья 13.14.** **Разглашение информации с ограниченным доступом**

Разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, -

влечет наложение административного штрафа

на граждан в размере **от 5 000 до одной 10 000** рублей;

на должностных лиц - **от 40 000 до 50 000** рублей,

на юридических лиц - **от 100 000 до 200 000 рублей**.

**Статья 5.39.** **Отказ в предоставлении гражданину информации**

Неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредоставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации –

влечет наложение административного штрафа на должностных лиц в размере **от 5 000 до 10 000 рублей**.

**Уголовный кодекс Российской Федерации**

**Статья 140. Отказ в предоставлении гражданину информации**

Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан, -

штраф **до 200 000** рублей или в размере дохода осужденного за период до 18 месяцев либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет.

**Статья 137. Нарушение неприкосновенности частной жизни**

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации -

штраф **до 200 000** рублей, лишение свободы на срок **до 2 лет**

2. Те же деяния, совершенные лицом с использованием своего служебного положения,

штраф **от 100 000 до 300 000** рублей, лишение свободы на срок **от 1 года до 4 лет**.

**Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений**

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан -

штраф **до 80 000** рублей, исправительные работы до 1 года.

2. То же деяние, совершенное лицом с использованием служебного положения или специальных технических средств, предназначенных для негласного получения информации, -

штраф **от 100 000 до 300 000** рублей, лишение свободы на срок **от 1 года до 4 лет**.

3. Незаконные производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации, -

штраф **до 200 000** рублей, лишение свободы на срок **до 3 лет.**

**Стандарты и технические спецификации в области информационной безопасности**

Различают **оценочные стандарты**, направленные на классификацию информационных систем и средств защиты по требованиям безопасности и **технические спецификации**, регламентирующие различные аспекты реализации средств защиты.

### "Оранжевая книга" как оценочный стандарт

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США **"Критерии оценки доверенных компьютерных систем".** Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года. Из его названия следует, что речь идет не о безопасных, а о доверенных системах, то есть системах, которым можно оказать определенную степень доверия.

"Оранжевая книга" дает **понятие безопасной системы**, которая "управляет, с помощью соответствующих средств доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию". Очевидно, что абсолютно безопасных систем не существует, поэтому есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

В "Оранжевой книге" **доверенная система** определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

В рассматриваемых Критериях безопасность и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической). Вопросы доступности "Оранжевая книга" не затрагивает.

**Степень доверия оценивается по двум основным критериям:**

1. **Политика безопасности** - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности - это **активный аспект защиты**, включающий в себя анализ возможных угроз и выбор мер противодействия.
2. **Уровень гарантированности** - мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это **пассивный аспект защиты**.

Из пассивных аспектов защиты в "Оранжевой книге" рассматривается два вида гарантированности - **операционная и технологическая**.

**Операционная гарантированность** относится к архитектурным и реализационным аспектам системы, технологическая - к методам построения и сопровождения. Операционная гарантированность включает в себя проверку следующих элементов:

* архитектура системы;
* целостность системы;
* проверка тайных каналов передачи информации;
* доверенное администрирование;
* доверенное восстановление после сбоев.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности.

**Технологическая гарантированность** охватывает весь жизненный цикл ИС, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные "закладки".

Важным средством обеспечения безопасности является **механизм протоколирования**. Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть **анализом регистрационной информации**.

**Доверенная вычислительная база** - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор. Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности.

Основное назначение доверенной вычислительной базы - выполнять функции **монитора обращений**, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

1. **Изолированность.** Необходимо предупредить возможность отслеживания работы монитора.
2. **Полнота.** Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.
3. **Верифицируемость.** Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать.

Реализация монитора обращений называется **ядром безопасности**. Ядро безопасности - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют **периметром безопасности**. Как уже указывалось, компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, - нет.

#### Механизмы безопасности

Согласно "Оранжевой книге", политика безопасности должна обязательно включать в себя следующие элементы:

* произвольное управление доступом;
* безопасность повторного использования объектов;
* метки безопасности;
* принудительное управление доступом.

**Произвольное управление доступом** (называемое иногда дискреционным) - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

**Безопасность повторного использования объектов** - важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

**Метки безопасности** состоят из двух частей - уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории - неупорядоченное. Назначение последних - описать предметную область, к которой относятся данные. Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта - степень конфиденциальности содержащейся в нем информации.

**Принудительное (или мандатное) управление доступом** (зависит от воли субъектов) основано на сопоставлении меток безопасности субъекта и объекта. После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта.

Если понимать политику безопасности как правила разграничения доступа, то механизм подотчетности является дополнением подобной политики. **Цель подотчетности** - в каждый момент времени знать, кто работает в системе и что делает. Средства подотчетности делятся на три категории:

* идентификация и аутентификация;
* предоставление доверенного пути;
* анализ регистрационной информации.

Обычный способ идентификации - ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности (аутентификации) пользователя - пароль.

Доверенный путь связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие, потенциально опасные компоненты ИС. Цель предоставления доверенного пути - дать пользователю возможность убедиться в подлинности обслуживающей его системы.

"Оранжевая книга" предусматривает наличие средств выборочного протоколирования, как в отношении пользователей, так и в отношении событий.

#### Классы безопасности

"Оранжевая книга" Министерства обороны США открыла путь к ранжированию информационных систем по степени доверия безопасности.

В "Оранжевой книге" определяется **четыре уровня доверия** - D, C, B и A:

* уровень C - произвольное управление доступом;
* уровень B - принудительное управление доступом;
* уровень A - верифицируемая безопасность.

Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Всего имеется **шесть классов безопасности** - C1, C2, B1, B2, B3, A1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, ее политика безопасности и уровень гарантированности должны удовлетворять заданным требованиям.

Например, требования к ИС согласно классу C1:

* доверенная вычислительная база должна управлять доступом именованных пользователей к именованным объектам;
* пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые доверенной вычислительной базой. Для аутентификации должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа;
* доверенная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы;
* должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;
* защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации. Тестирование должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты доверенной вычислительной базы;
* должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации доверенной вычислительной базы.

Публикация "Оранжевой книги" стала событием в области информационной безопасности. Появился общепризнанный понятийный базис, без которого даже обсуждение проблем ИБ было бы затруднительным.

### Информационная безопасность распределенных систем. Рекомендации X.800

#### Сетевые сервисы безопасности

Техническая спецификация X.800 появилась несколько позднее "Оранжевой книги", но весьма полно и глубоко трактует вопросы информационной безопасности распределенных систем. В ней можно выделить специфические сетевые функции (сервисы) безопасности, а также необходимые для их реализации защитные механизмы.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

1. **Аутентификация**. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).
2. **Управление доступом**. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.
3. **Конфиденциальность данных**. Обеспечивает защиту от несанкционированного получения информации. Отдельно стоит упомянуть **конфиденциальность трафика** (это защита информации, которую можно получить, анализируя сетевые потоки данных).
4. **Целостность данных** подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.
5. **Неотказуемость** (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.

#### Сетевые механизмы безопасности

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

1. **шифрование**;
2. **электронная цифровая подпись**;
3. **механизмы управления доступом**. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
4. **механизмы контроля целостности данных.** В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;
5. **механизмы аутентификации**. Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
6. **механизмы** **дополнения трафика** (выработка и поддержание правил, задающих характеристики дополняющих сообщений - частоту отправки, размер и т.п.);
7. **механизмы управления маршрутизацией**. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;
8. **механизмы нотаризации**. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

#### Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение криптографических ключей, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждая из оконечных систем должна располагать информацией, необходимой для реализации избранной политики безопасности.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

* администрирование информационной системы в целом;
* администрирование сервисов безопасности;
* администрирование механизмов безопасности.

Среди действий, относящихся к ИС в целом, отметим обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов.

Администрирование средств безопасности в распределенной ИС имеет много особенностей по сравнению с централизованными системами.

### "Общие критерии оценки безопасности информационных технологий"

Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. По историческим причинам данный стандарт часто называют **"Общими критериями"** (или даже ОК). Под ОК можно с некоторой оговоркой подразумевать и стандарт ISO/IEC 15408-1,2,3-2005 (ГОСТ Р ИСО/МЭК 15408-1,2,3-2008).

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от "Оранжевой книги", ОК не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные "программы" - **задания по безопасности**, **типовые профили защиты** и т.п. Как и "Оранжевая книга", ОК содержат два основных вида требований безопасности:

* **функциональные**, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
* **требования доверия**, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

ОК состоят из трех частей:

- часть 1. Введение и общая модель;

- часть 2. Функциональные требования безопасности;

- часть 3. Требования доверия к безопасности.

Требования безопасности предъявляются, а их выполнение проверяется для определенного **объекта оценки** - аппаратно-программного продукта или информационной системы.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

* определение назначения, условий применения, целей и требований безопасности;
* проектирование и разработка;
* испытания, оценка и сертификация;
* внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте **среды безопасности**, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

* источник угрозы;
* метод воздействия;
* уязвимые места, которые могут быть использованы;
* ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в:

* требованиях безопасности;
* проектировании;
* эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

С точки зрения технологии программирования в ОК использован устаревший библиотечный (не объектный) подход. Чтобы структурировать пространство требований, в "Общих критериях" введена иерархия **класс-семейство-компонент-элемент**:

1. **Классы** определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).
2. **Семейства** в пределах класса различаются по строгости и другим нюансам требований.
3. **Компонент** - минимальный набор требований, фигурирующий как целое.
4. **Элемент** - неделимое требование.

Как и между библиотечными функциями, между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения **цели безопасности**. Вообще говоря, не все комбинации компонентов имеют смысл, и понятие зависимости в какой-то степени компенсирует недостаточную выразительность библиотечной организации, хотя и не заменяет объединение функций в содержательные объектные интерфейсы. С помощью библиотек могут формироваться два вида нормативных документов: профиль защиты и задание по безопасности.

**Профиль защиты** (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

**Задание по безопасности** содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

В ОК нет готовых классов защиты. Сформировать классификацию в терминах "Общих критериев" - значит определить несколько иерархически упорядоченных профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

Выделение некоторого подмножества из всего множества профилей защиты во многом носит субъективный характер. По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода) целесообразно сформировать сначала отправную точку классификации, выделив базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

**Функциональный пакет** - это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. "Общие критерии" не регламентируют структуру пакетов, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения.

#### Функциональные требования

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов. Перечислим классы функциональных требований ОК:

1. **идентификация и аутентификация**;
2. **защита данных пользователя**;
3. **защита функций безопасности** (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
4. **управление безопасностью** (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
5. **аудит безопасности** (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
6. **доступ к объекту оценки**;
7. **приватность** (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
8. **использование ресурсов** (требования к доступности информации);
9. **криптографическая поддержка** (управление ключами);
10. **связь** (аутентификация сторон, участвующих в обмене данными);
11. **доверенный маршрут/канал** (для связи с сервисами безопасности).

Например, класс "Приватность" содержит 4 семейства функциональных требований:

1. **Анонимность**. Позволяет выполнять действия без раскрытия идентификатора пользователя другим пользователям, субъектам и/или объектам. Анонимность может быть полной или выборочной. В последнем случае она может относиться не ко всем операциям и/или не ко всем пользователям (например, у уполномоченного пользователя может оставаться возможность выяснения идентификаторов пользователей).
2. **Псевдонимность**. Напоминает анонимность, но при применении псевдонима поддерживается ссылка на идентификатор пользователя для обеспечения подотчетности или для других целей.
3. **Невозможность ассоциации**. Семейство обеспечивает возможность неоднократного использования информационных сервисов, но не позволяет ассоциировать случаи использования между собой и приписать их одному лицу. Невозможность ассоциации защищает от построения профилей поведения пользователей (и, следовательно, от получения информации на основе подобных профилей).
4. **Скрытность**. Требования данного семейства направлены на то, чтобы можно было использовать информационный сервис с сокрытием факта использования. Для реализации скрытности может применяться, например, широковещательное распространение информации, без указания конкретного адресата. Годятся для реализации скрытности и методы стеганографии, когда скрывается не только содержание сообщения (как в криптографии), но и сам факт его отправки.

Класс "Использование ресурсов", содержащий требования доступности, включает три семейства:

1. **Отказоустойчивость**. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В ОК различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.
2. **Обслуживание по приоритетам**. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.
3. **Распределение ресурсов**. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

"Общие критерии" - продуманный и полный документ с точки зрения функциональных требований, однако в нем есть и некоторые недостатки, главный из которых - отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. В "Общих критериях" отсутствуют архитектурные требования, что является естественным следствием избранного подхода "снизу вверх".

#### Требования доверия безопасности

Установление доверия безопасности, согласно "Общим критериям", основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

1. действия разработчиков;
2. представление и содержание свидетельств;
3. действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

1. разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
2. поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
3. тестирование;
4. оценка уязвимостей (включая оценку стойкости функций безопасности);
5. поставка и эксплуатация;
6. управление конфигурацией;
7. руководства (требования к эксплуатационной документации);
8. поддержка доверия (для поддержки этапов жизненного цикла после сертификации);
9. оценка профиля защиты;
10. оценка задания по безопасности.

Применительно к требованиям доверия в "Общих критериях" введены так называемые оценочные уровни доверия (семь), содержащие осмысленные комбинации компонентов:

1. Предусматривает анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.
2. В дополнение к первому уровню, предусматривает наличие проекта верхнего уровня объекта оценки, выборочное независимое тестирование, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.
3. Ведется контроль среды разработки и управление конфигурацией объекта оценки.
4. Добавляются полная спецификация интерфейсов, проекты нижнего уровня, анализ подмножества реализации, применение неформальной модели политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.
5. Предусматривает применение формальной модели политики безопасности, полуформальных функциональной спецификации и проекта верхнего уровня с демонстрацией соответствия между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.
6. Реализация должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.
7. Предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

### Руководящие документы ФСТЭК

ФСТЭК России ведет активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления ФСТЭК России выбрала ориентацию на «Общие критерии».

Список нормативных документов:

1. РД. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
2. РД. Защита от несанкционированного доступа к информации. Термины и определения.
3. РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
4. РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
5. РД. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.
6. РД. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.
7. РД. Защита информации. Специальные защитные знаки. Классификация и общие требования
8. РД. Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации. Сборник руководящих документов по защите информации от несанкционированного доступа.
9. РД. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей
10. РД. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. (Часть 1,   Часть 2,    Часть3).
11. РД. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности
12. РД. Безопасность информационных технологий. Руководство по регистрации профилей защиты
13. РД. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты.
14. Руководство по разработке профилей защиты и заданий по безопасности.
15. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
16. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных.
17. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
18. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных(выписка).
19. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
20. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
21. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
22. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
23. ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.
24. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.
25. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Ведение и общая модель.
26. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
27. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
28. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
29. ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации».
30. ГОСТ Р ИСО ТО 13569 «Финансовые услуги. Рекомендации по информационной безопасности».
31. ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3.
32. ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».
33. ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».
34. ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».
35. ГОСТ Р ИСО/МЭК 27006 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».
36. ГОСТ Р ИСО/МЭК 18028-1 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности».
37. ГОСТ Р ИСО/МЭК ТО 24762 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».
38. ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации».

**РД. Классификация автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД).**

В РД описываются 9 классов защищенности АС. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности.

Группа содержит два класса - 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Таблица 1 Требования к защищенности автоматизированных систем** | | | | | | | | | |
| **Подсистемы и требования** | **Классы** | | | | | | | | |
| **3Б** | **3А** | **2Б** | **2А** | **1Д** | **1Г** | **1В** | **1Б** | **1А** |
| 1. Подсистема управления доступом 1.1. Идентификация, проверка подлинности и контроль доступа субъектов: в систему; | + | + | + | + | + | + | + | + | + |
| к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ; | - | - | - | + | - | + | + | + | + |
| к программам; | - | - | - | + | - | + | + | + | + |
| к томам, каталогам, файлам, записям, полям записей. | - | - | - | + | - | + | + | + | + |
| 1.2. Управление потоками информации | - | - | - | + | - | - | + | + | + |
| 2. Подсистема регистрации и учета 2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети); | + | + | + | + | + | + | + | + | + |
| выдачи печатных (графических) выходных документов; | - | + | - | + | - | + | + | + | + |
| запуска/завершения программ и процессов (заданий, задач); | - | - | - | + | - | + | + | + | + |
| доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей; | - | - | - | + | - | + | + | + | + |
| изменения полномочий субъектов доступа; | - | - | - | - | - | - | + | + | + |
| создаваемых защищаемых объектов доступа. | - | - | - | + | - | - | + | + | + |
| 2.2. Учет носителей информации. | + | + | + | + | + | + | + | + | + |
| 2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. | - | + | - | + | - | + | + | + | + |
| 2.4. Сигнализация попыток нарушения защиты. | - | - | - | - | - | - | + | + | + |
| 3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации. | - | - | - | + | - | - | - | + | + |
| 3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах. | - | - | - | - | - | - | - | - | + |
| 3.3. Использование аттестованных (сертифицированных) криптографических средств. | - | - | - | + | - | - | - | + | + |
| 4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации. | + | + | + | + | + | + | + | + | + |
| 4.2. Физическая охрана средств вычислительной техники и носителей информации. | + | + | + | + | + | + | + | + | + |
| 4.3. Наличие администратора (службы защиты) информации в АС. | - | - | - | + | - | - | + | + | + |
| 4.4. Периодическое тестирование СЗИ НСД. | + | + | + | + | + | + | + | + | + |
| 4.5. Наличие средств восстановления СЗИ НСД. | + | + | + | + | + | + | + | + | + |
| 4.6. Использование сертифицированных средств защиты. | - | + | - | + | - | - | + | + | + |

"СЗИ НСД" система защиты информации от несанкционированного доступа

### Административный уровень обеспечения ИБ

К **административному уровню информационной безопасности** относятся действия общего характера, предпринимаемые руководством организации. Главная цель мер административного уровня - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. **Под политикой безопасности** понимается совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется **программа обеспечения информационной безопасности**. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

* решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
* формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
* обеспечение базы для соблюдения законов и правил;
* формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

**Для политики безопасности верхнего уровня** цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

**Политика безопасности среднего уровня** должна для каждого аспекта освещать следующие темы:

1. **Описание аспекта.** Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.
2. **Область применения.** Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?
3. **Роли и обязанности**. В документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.
4. **Законопослушность**. Политика должна содержать общее описание запрещенных действий и наказаний за них.
5. **Точки контакта**. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией.

**Политика безопасности нижнего уровня** относится к конкретным информационным сервисам. Она включает в себя два аспекта - **цели и правила их достижения**, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

* кто имеет право доступа к объектам, поддерживаемым сервисом?
* при каких условиях можно читать и модифицировать данные?
* как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей.

### Программа безопасности

**Британский стандарт BS 7799:1995** рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

* вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
* организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
* классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
* штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
* раздел, освещающий вопросы физической защиты;
* управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
* раздел, описывающий правила разграничения доступа к производственной информации;
* раздел, характеризующий порядок разработки и сопровождения систем;
* раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
* юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней - верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

* управление рисками (оценка рисков, выбор эффективных средств защиты);
* координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;
* стратегическое планирование;
* контроль деятельности в области информационной безопасности.

**В рамках программы безопасности верхнего** уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

**Цель программы безопасности нижнего уровня** - обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

### Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее.

В жизненном цикле информационного сервиса можно выделить следующие этапы:

1. **Инициация.** На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение, определяется, какими характеристиками и какой функциональностью он должен обладать, оцениваются финансовые и иные ограничения.
2. **Закупка.** Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.
3. **Установка.** Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию. Полнота и комплексность тестирования могут служить гарантией безопасности эксплуатации в штатном режиме.
4. **Эксплуатация.** На данном этапе сервис не только работает и администрируется, но и подвергается модификациям. Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. После значительных модификаций подобные проверки являются обязательными.
5. **Выведение из эксплуатации.** Происходит переход на новый сервис. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. При выведении данных из эксплуатации их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. При архивировании необходимо позаботиться о восстановимости данных.

**Управление рисками**

Управление рисками рассматривается на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Управление рисками, равно как и выработка собственной политики безопасности, актуально только для тех организаций, информационные системы которых и/или обрабатываемые данные можно считать нестандартными. Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

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

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

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

По отношению к выявленным рискам возможны следующие действия:

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

Процесс управления рисками можно разделить на следующие этапы:

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

Управление рисками - процесс циклический. Риски нужно контролировать постоянно, периодически проводя их переоценку. Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС.

Выбор анализируемых объектов и уровня детализации их рассмотрения - первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки.

Очень важно выбрать разумную **методологию оценки рисков**. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства стоит использовать. Управление рисками - типичная оптимизационная задача. Принципиальная трудность состоит в неточности исходных данных. В простейшем и вполне допустимом случае можно пользоваться трехбалльной шкалой.

**При идентификации активов** следует учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации. Отправной точкой здесь является представление о миссии организации, то есть об основных направлениях деятельности, которые желательно сохранить в любом случае. Одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее использования. Эти сведения целесообразно нанести на карту ИС в качестве граней соответствующих объектов.

Информационной основой сколько-нибудь крупной организации является сеть, поэтому в число аппаратных активов следует включить компьютеры (серверы, рабочие станции, ПК), периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование (мосты, маршрутизаторы и т.п.). К программным активам, вероятно, будут отнесены операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, средства управления сетью и отдельными системами. Важно зафиксировать, где (в каких узлах сети) хранится программное обеспечение, и из каких узлов оно используется. Третьим видом информационных активов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, способы доступа к ним.

Анализ угроз и их последствий, выявление уязвимых мест в защите. Первый шаг в анализе угроз - их идентификация. Целесообразно выявлять не только сами угрозы, но и источники их возникновения - это поможет в выборе дополнительных средств защиты. Например, нелегальный вход в систему может стать следствием воспроизведения начального диалога, подбора пароля или подключения к сети неавторизованного оборудования. Очевидно, для противодействия каждому из перечисленных способов нелегального входа нужны свои механизмы безопасности.

**Оценка рисков.** После идентификации угрозы необходимо оценить вероятность ее осуществления (например, по трехбалльной шкале - низкая (1), средняя (2) и высокая (3) вероятность). Кроме вероятности осуществления, важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трехбалльной шкале.

Вполне допустимо применить такой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб. Если для вероятности и ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и четвертый - к среднему, два последних - к высокому, после чего появляется возможность снова привести их к трехбалльной шкале. По этой шкале и следует оценивать приемлемость рисков.

### Процедурный уровень обеспечения ИБ

На процедурном уровне можно выделить следующие классы мер:

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

**Управление персоналом**

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше - с составления описания должности. Существует два общих принципа, которые следует иметь в виду:

* разделение обязанностей;
* минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, нежелательна ситуация, когда крупные платежи от имени организации выполняет один человек. Надежнее поручить одному сотруднику оформление заявок на подобные платежи, а другому - заверять эти заявки. Другой пример - процедурные ограничения действий суперпользователя. Можно искусственно "расщепить" пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую - другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоем, что снижает вероятность ошибок и злоупотреблений.

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно - уменьшить ущерб от случайных или умышленных некорректных действий.

Предварительное составление описания должности позволяет оценить ее критичность и спланировать процедуру проверки и отбора кандидатов. Когда кандидат определен, он, вероятно, должен пройти обучение; по крайней мере, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до заведения его системного счета с входным именем, паролем и привилегиями.

С момента заведения системного счета начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности и т.п. Все это требует соответствующего изменения привилегий. Техническую сложность представляют временные перемещения пользователя, выполнение им обязанностей взамен сотрудника, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала предоставить, а через некоторое время взять обратно.

Проблема обучения - одна из основных с точки зрения информационной безопасности. Если сотрудник не знаком с политикой безопасности своей организации, он не может стремиться к достижению сформулированных в ней целей. Напротив, если сотрудник знает, что его действия протоколируются, он, возможно, воздержится от нарушений.

**Физическая защита**

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных.

Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как "непрерывность защиты в пространстве и времени". Ранее мы рассматривали понятие окна опасности. Для физической защиты таких окон быть не должно.

Существуют следующие направления физической защиты:

* физическое управление доступом;
* противопожарные меры;
* защита поддерживающей инфраструктуры;
* защита от перехвата данных;
* защита мобильных систем.

Перехват данных может осуществляться самыми разными способами. Злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, производить анализ побочных электромагнитных излучений и наводок и т.д.

**Поддержка программного обеспечения** - одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо следить за тем, какое программное обеспечение установлено на компьютерах. Если пользователи будут устанавливать программы по своему усмотрению, это может привести к заражению вирусами, а также появлению утилит, действующих в обход защитных средств.

Второй аспект поддержки программного обеспечения - контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Сюда можно отнести поддержку эталонных копий программных систем. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и обеспечения целостности.

Лучший способ уменьшить количество ошибок в рутинной работе - максимально автоматизировать ее. Резервное копирование необходимо для восстановления программ и данных после аварий. Нужно также обеспечить сохранность копий.

Документирование - неотъемлемая часть информационной безопасности. В виде документов оформляется почти все - от политики безопасности до журнала учета носителей. К хранению одних документов (содержащих, например, анализ уязвимых мест системы и угроз) применимы требования обеспечения конфиденциальности, к другим, таким как план восстановления после аварий - требования целостности и доступности (в критической ситуации план необходимо найти и прочитать).

Регламентные работы - очень серьезная угроза безопасности. Сотрудник, осуществляющий регламентные работы, получает исключительный доступ к системе, и на практике очень трудно проконтролировать, какие именно действия он совершает. Здесь на первый план выходит степень доверия к тем, кто выполняет работу.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием выявить нарушителя. В политике безопасности организации приоритеты должны быть расставлены заранее. Поскольку, как показывает практика, выявить злоумышленника очень сложно, в первую очередь следует заботиться об уменьшении ущерба.

**Планирование восстановительных работ**

Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объеме.

Меры информационной безопасности можно разделить на три группы, в зависимости от того, направлены ли они на предупреждение, обнаружение или ликвидацию последствий атак.

Процесс планирования восстановительных работ можно разделить на следующие этапы:

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

Планируя восстановительные работы, следует отдавать себе отчет в том, что полностью сохранить функционирование организации не всегда возможно. Необходимо выявить критически важные функции, без которых организация теряет свое лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить работу после аварии.

**Программно-технический уровень обеспечения ИБ**

**Программно-технические меры**, то есть меры, направленные на контроль компьютерных сущностей - оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности. Ущерб наносят в основном действия легальных пользователей, по отношению к которым процедурные регуляторы малоэффективны. Главные враги - некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

Центральным для программно-технического уровня является **понятие сервиса безопасности.**

Следуя объектно-ориентированному подходу, при рассмотрении информационной системы с единичным уровнем детализации мы увидим совокупность предоставляемых ею информационных сервисов. Назовем их основными. Чтобы они могли функционировать и обладали требуемыми свойствами, необходимо несколько уровней дополнительных (вспомогательных) сервисов - от СУБД и мониторов транзакций до ядра операционной системы и оборудования.

К вспомогательным относятся следующие сервисы безопасности:

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

Совокупность перечисленных выше сервисов безопасности будет называться полным набором. Считается, что его достаточно для построения надежной защиты на программно-техническом уровне при соблюдении целого ряда дополнительных условий (отсутствие уязвимых мест, безопасное администрирование и т.д.).

Для проведения классификации сервисов безопасности и определения их места в общей архитектуре меры безопасности можно разделить на следующие виды:

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