**Информационная безопасность**

***Информационная безопасность*** — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере.

***Информационная безопасность*** – это процесс обеспечения конфиденциальности, целостности и доступности информации.

*Конфиденциальность*: Обеспечение доступа к информации только авторизованным пользователям.

*Целостность*: Обеспечение достоверности и полноты информации и методов ее обработки.

*Доступность*: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Сегодня используется шесть **основных способов защиты**: Препятствие; Маскировка; Регламентация; Управление; Принуждение; Побуждение. Все перечисленные методы нацелены на построение эффективной технологии защиты информации, при которой исключены потери по причине халатности и успешно отражаются разные виды угроз.

Под препятствием понимается способ физической защиты информационных систем, благодаря которому злоумышленники не имеют возможность попасть на охраняемую территорию. Маскировка — способы защиты информации, предусматривающие преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа. Управление — способы защиты информации, при которых осуществляется управление над всеми компонентами информационной системы. Регламентация — важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными. Принуждение — методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Если используются способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям, то речь идет о побуждении.

Способы защиты информации предполагают использование определенного набора средств. Для предотвращения потери и утечки секретных сведений. Используются следующие **средства**: Физические; Программные и аппаратные; Организационные; Законодательные; Психологические.

Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основным и наиболее старым средством физического препятствия является установка прочных дверей, надежных замков, решеток на окна. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка противопожарной системы. Физические средства используются для охраны данных как на бумажных, так и на электронных носителях. Программные и аппаратные средства — незаменимый компонент для обеспечения безопасности современных информационных систем. Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации. Программные средства — программы, отражающие хакерские атаки. Также к программным средствам можно отнести программные комплексы, выполняющие восстановление утраченных сведений. При помощи комплекса аппаратуры и программ обеспечивается резервное копирование информации — для предотвращения потерь. Организационные средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных. Законодательные средства — комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации. Психологические средства — комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К психологическим средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе предприятия.

 Для обеспечения безопасности информационных систем сегодня активно используются **методы шифрования** и защиты электронных документов. Данные технологии позволяют осуществлять удаленную передачу данных и удаленное подтверждение подлинности. Методы защиты информации путем шифрования (криптографические) основаны на изменении информации с помощью секретных ключей особого вида. В основе технологии криптографии электронных данных — алгоритмы преобразования, методы замены, алгебра матриц. Стойкость шифрования зависит от того, насколько сложным был алгоритм преобразования. Зашифрованные сведения надежно защищены от любых угроз, кроме физических. Электронная цифровая подпись (ЭЦП) — параметр электронного документа, служащий для подтверждения его подлинности. Электронная цифровая подпись заменяет подпись должностного лица на бумажном документе и имеет ту же юридическую силу. ЭЦП служит для идентификации ее владельца и для подтверждения отсутствия несанкционированных преобразований. Использование ЭЦП обеспечивает не только защиту информации, но также способствует удешевлению технологии документооборота, снижает время движения документов при оформлении отчетов.

 Используемая технология защиты и степень ее эффективности определяют **класс** **безопасности информационной системы**. В международных стандартах выделяют 7 классов безопасности систем, которые объединены в 4 уровня: D — нулевой уровень безопасности; С — системы с произвольным доступом; В — системы с принудительным доступом; А — системы с верифицируемой безопасностью.

 Уровню D соответствуют системы, в которых слабо развита технология защиты. При такой ситуации любое постороннее лицо имеет возможность получить доступ к сведениям. Использование слаборазвитой технологии защиты чревато потерей или утратой сведений. В уровне С есть следующие классы — С1 и С2. Класс безопасности С1 предполагает разделение данных и пользователей. Определенная группа пользователей имеет доступ только к определенным данным, для получения сведений необходима аутентификация — проверка подлинности пользователя путем запроса пароля. При классе безопасности С1 в системе имеются аппаратные и программные средства защиты. Системы с классом С2 дополнены мерами, гарантирующими ответственность пользователей: создается и поддерживается журнал регистрации доступа. Уровень В включает технологии обеспечения безопасности, которые имеют классы уровня С, плюс несколько дополнительных. Класс В1 предполагает наличие политики безопасности, доверенной вычислительной базы для управления метками безопасности и принудительного управления доступом. При классе В1 специалисты осуществляют тщательный анализ и тестирование исходного кода и архитектуры. Класс безопасности В2 характерен для многих современных систем и предполагает: Снабжение метками секретности всех ресурсов системы; Регистрацию событий, которые связаны с организацией тайных каналов обмена памятью; Структурирование доверенной вычислительной базы на хорошо определенные модули; Формальную политику безопасности; Высокую устойчивость систем к внешним атакам. Класс В3 предполагает, в дополнение к классу В1, оповещение администратора о попытках нарушения политики безопасности, анализ появления тайных каналов, наличие механизмов для восстановления данных после сбоя в работе аппаратуры или программного обеспечения. Уровень А включает один, наивысший класс безопасности — А. К данному классу относятся системы, прошедшие тестирование и получившие подтверждение соответствия формальным спецификациям верхнего уровня.

Множество существующих методов обеспечения информационной безопасности можно классифицировать по разным признакам, но только уместные комбинации этих признаков позволяют сетевому администратору обеспечить надлежащий уровень информационной безопасности.
В целом все методы можно разделить на два класса:

1. Организационно - правовые методы, включающие воспитание у пользователей отношение недоступности и нетерпимости к нарушению информационной безопасности.
2. Организационно - технические методы.

Перечислим ***основные методы обеспечения информационной безопасности***:

1. *Авторизация.*
Этот метод позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.
2. *Идентификация и аутентификация*.
Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д. Последние годы активно внедряются следующие методы аутентификации:
	1. Биометрия. Используется аутентификация по геометрии руки, радужной оболочки сетчатки глаза, клавиатурный почерк, отпечатки глаза и т.п.
	2. SMART-карты (интеллектуальные карты). Их удобство заключается в портативном и широком спектре функций, которые могут быть легко модифицированы. Недостатком SMART-карты является их дороговизна, так как требуют определенных устройств для считывания информации.
	3. е-Token (электронный ключ) – аналог SMART-карты, выполненный в виде брелка, подключающегося через USB-порт. Достоинство e-Token заключается в том, что он не требует специальных, дорогостоящих карт -reader.
	4. определение координат пользователя.
		* GPS- глобальная система позиционирования
		* Система GSM. (100-300м).
	5. Криптография.
3. *Протоколирование и аудит*.
4. *Экранирование* – разделение информационных потоков между различными информационными системами.
5. *Физическая защита*. Администратору сети необходимо знать все возможные точки физического проникновения в сеть или нанесения ущерба. Физические устройства защиты:
	1. Физические устройства доступности к сетевым узлам и линиям связи.
	2. Противопожарные меры
	3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
	4. Защита мобильных и радио систем.
	5. Защита от перехвата данных.
6. *Поддержка текущей работоспособности.*
	1. Резервное копирование.
	2. Управление носителями.
	3. Регламентированные работы.

*Под информационной безопасностью Российской Федерации* понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных социальных интересов личности, общества и государства.

Интересы государства в информационной сфере заключаются в использовании информации и информационной инфраструктуры для обеспечения государственной политики, защиты нравственных ценностей общества, поддержания устойчивого функционирования информационной инфраструктуры, управления делами общества. Национальные интересы в информационной сфере определяются прежде всего той ролью, которую играют информация, информационные технологии и созданная на их базе информационная инфраструктура в сохранении национальной идентичности и обеспечении устойчивого развития нации в конкретных исторических условиях.

Информационная безопасность — одна из наиболее важных задач в информационной сфере Российской Федерации. Обеспечение информационной безопасности Российской Федерации достигается посредством разработки и реализации комплекса мероприятий, направленных на поддержание состояния защищенности национальных интересов Российской Федерации в различных сферах жизни и деятельности общества и государства. Особое место в системе этих мероприятий занимают организационные меры, способы и методы обеспечения информационной безопасности.

Защита информационных ресурсов предприятия включает деятельность руководства, должностных лиц и структурных подразделений предприятия по принятию правовых, организационных и технических мер, направленных на:
*- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;*
*- соблюдение конфиденциальности информации ограниченного доступа;*
*- реализацию права на доступ к информации.*

Особую роль в системе средств обеспечения информационной безопасности играют организационные средства, к ним относятся:
*1. средства кадрового обеспечения —* совокупность программ подготовки кадров по направлениям информационной безопасности и используемого в процессе подготовки учебного и методического материала ;
2. *средства материального обеспечения* — совокупность объектов, выделяемых для размещения и использования сил и средств обеспечения информационной безопасности;
3. *средства финансового обеспечения информационной безопасности* — экономические инструменты получения и использования денежных средств для решения поставленных задач;
4. *средства информационного обеспечения* — информационные ресурсы (информационные фонды, банки данных), используемые при решении задач обеспечения информационной безопасности;
5. *средства научного обеспечения информационной безопасности* — система научных теорий, концепций, взглядов и закономерностей, предназначенных для изучения происходящих в данной области процессов и явлений, анализа угроз и выработки способов и методов противодействия этим угрозам.

Наряду с перечисленными организационными средствами в общей системе обеспечения информационной безопасности важное место занимают и организационные методы:
*1- создание и совершенствование системы обеспечения информационной безопасности ;*
*2- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;*
*3- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;*
*4- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;*
*5- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;*
*6- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.*

**Методы защиты информации**

Защита информации в компьютерных системах обеспечивается созданием комплексной системы защиты. Комплексная система защиты включает:

* правовые методы защиты;
* организационные методы защиты;
* методы защиты от случайных угроз;
* методы защиты от традиционного шпионажа и диверсий;
* методы защиты от электромагнитных излучений и наводок;
* методы защиты от несанкционированного доступа;
* криптографические методы защиты;
* методы защиты от компьютерных вирусов.

Среди методов защиты имеются и универсальные, которые являются базовыми при создании любой системы защиты. Это, прежде всего, правовые методы защиты информации, которые служат основой легитимного построения и использования системы защиты любого назначения. К числу универсальных методов можно отнести и организационные методы, которые используются в любой системе защиты без исключений и, как правило, обеспечивают защиту от нескольких угроз.

Методы защиты от случайных угроз разрабатываются и внедряются на этапах проектирования, создания, внедрения и эксплуатации  компьютерных систем. К их числу относятся:

* создание высокой надёжности компьютерных систем;
* создание отказоустойчивых компьютерных систем;
* блокировка ошибочных операций;
* оптимизация взаимодействия пользователей и обслуживающего персонала с компьютерной системой;
* минимизация ущерба от аварий и стихийных бедствий;
* дублирование информации.

При защите информации в компьютерных системах от традиционного шпионажа и диверсий используются те же средства и методы защиты, что и для защиты других объектов, на которых не используются компьютерные системы. К их числу относятся:

* создание системы охраны объекта;
* организация работ с конфиденциальными информационными ресурсами;
* противодействие наблюдению и подслушиванию;
* защита от злоумышленных действий персонала.

Все методы защиты от электромагнитных излучений и наводок можно разделить на пассивные и активные. Пассивные методы обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов. Активные методы защиты направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих приём и выделение полезной информации из перехваченных злоумышленником сигналов. На электронные блоки и магнитные запоминающие устройства могут воздействовать мощные внешние электромагнитные импульсы и высокочастотные излучения. Эти воздействия могут приводить к неисправности электронных блоков и стирать информацию с магнитных носителей информации.  Для блокирования угрозы такого воздействия используется  экранирование защищаемых средств.

Для защиты информации от несанкционированного доступа создаются:

* система разграничения доступа к информации;
* система защиты от исследования и копирования программных средств.

Исходной информацией для создания системы разграничения доступа является решение администратора компьютерной системы о допуске пользователей к определённым информационным ресурсам. Так как информация в компьютерных системах хранится, обрабатывается и передаётся файлами (частями файлов), то доступ к информации регламентируется на уровне файлов. В базах данных доступ может регламентироваться к отдельным её частям по определённым правилам. При определении полномочий доступа администратор устанавливает операции, которые разрешено выполнять пользователю. Различают следующие операции с файлами:

* чтение (R);
* запись;
* выполнение программ (E).

Операции записи имеют две модификации:

* субъекту доступа может быть дано право осуществлять запись с изменением содержимого файла (W);
* разрешение дописывания в файл без изменения старого содержимого (A).

Система защиты от исследования и копирования программных средств включает следующие методы:

* методы, затрудняющие считывание скопированной информации;
* методы, препятствующие использованию информации.

  Под криптографической защитой информации понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий. По виду воздействия на исходную информацию методы криптографического преобразования информации разделяются на следующие группы:

* шифрование;
* стенография;
* кодирование;
* сжатие.