**Лекция 1**

**ПОНЯТИЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

1. Понятие безопасности и жизненно важных интересов.
2. Определение информационной безопасности (ИБ) и информационной среды
3. Определение ИБ РФ (Доктрина информационной безопасности).
4. Виды угроз информационной безопасности Российской Федерации

**1. Понятие безопасности и жизненно важных интересов.**

**Безопасность** определяется как **состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.**

В свою очередь **жизненно важные интересы – это совокупность потребностей,** удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

**2.** **Определение информационной безопасности (ИБ) и информационной среды**

Понятие информационная безопасность в научной литературе сначала отождествлялось с понятием **безопасность информации**. Существует несколько определений понятия **безопасность информации**. Общий подход: **безопасность информации** **как состояние защищенности информации.** Это не вызывает возражений, ибо сам термин безопасность означает отсутствие опасностей,

Информационная (сфера) среда – сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информацииОпределение очень неконкретное.

**3. Определение ИБ РФ (Доктрина информационной безопасности).**

**В «Доктрине информационной безопасности РФ»** дано определение: **ИБ – это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.**

Жизненно важные интересы в информационной сфере:

**Интересы личности** в информационной сфере заключаются

* в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития,
* а также в защите информации, обеспечивающей личную безопасность.
* в защите права интеллектуальной собственности,
* обеспечение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации.

**Интересы общества** в информационной сфере заключаются:

* в обеспечении интересов личности в этой сфере,
* упрочении демократии, создании правового социального государства,
* достижении и поддержании общественного согласия, в духовном обновлении России.
* Бачило: Сохранение нравственных ценностей, утверждение в обществе идеалов высокой нравственности, патриотизма и гуманизма, развитие многовековых духовных традиций России, пропаганда национального культурного наследия, норм морали и общественной нравственности,
* предотвращение манипулирования массовым сознанием,
* приоритетное развитие современных телекоммуникационных технологий, сохранение и развитие отечесивенного научного и производственного потенциала.

**Интересы государства** в информационной сфере заключаются:

* в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности,
* в безусловном обеспечении законности и правопорядка,
* развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются **четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.**

**Первая составляющая** национальных интересов Российской Федерации в информационной сфере включает в себя **соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.**

Для достижения этого требуется:

* повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;
* усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;
* обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;
* обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
* укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
* гарантировать свободу массовой информации и запрет цензуры;
* не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;
* обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

**Вторая составляющая** национальных интересов Российской Федерации в информационной сфере включает в себя **информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.**

Для достижения этого требуется:

* укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;
* интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

**Третья составляющая** национальных интересов Российской Федерации в информационной сфере включает в себя **развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи,** обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

* развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;
* развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
* развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;
* обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

**Четвертая составляющая** национальных интересов Российской Федерации в информационной сфере включает в себя **защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем,** как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

* повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
* интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
* обеспечить защиту сведений, составляющих государственную тайну;
* расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

 Все составляющие национальных интересов РФ в информационной сфере, названные в Доктрине информационной безопасности РФ, - есть ключевые процессы информатизации общества.

# Виды угроз информационной безопасности Российской Федерации

По своей общей направленности **угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:**

* угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
* угрозы информационному обеспечению государственной политики Российской Федерации;
* угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
* угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

**Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России** могут являться:

* принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
* создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
* противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
* нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
* противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
* неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
* неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
* дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
* нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
* вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
* девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
* снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
* манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

* монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
* блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
* низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

**Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи,** обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

* противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
* закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
* вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
* увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

**Угрозами безопасности информационных и телекоммуникационных средств и систем**, как уже развернутых, так и создаваемых на территории России, могут являться:

* противоправные сбор и использование информации;
* нарушения технологии обработки информации;
* внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
* разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
* уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
* воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
* компрометация ключей и средств криптографической защиты информации;
* утечка информации по техническим каналам;
* внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
* уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
* перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
* использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
* несанкционированный доступ к информации, находящейся в банках и базах данных;
* нарушение законных ограничений на распространение информации.

**Литература:**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. Анин Б.Ю. Защита компьютерной информации. Петербург, 2010. - 384с.
4. Галатенко В.А. Барсуков В.С., Водолазний В.В. Современные технологии безопасности. - М.: «Нолидж», 2009. - 496 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
7. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция №2**

**Информационная безопасность в системе**

**национальной безопасности РФ**

1. Классификация видов безопасности.
2. Понятие «национальная безопасность».
3. Основные положения «Концепции национальной безопасности РФ».

**1. Классификация видов безопасности.**

**Безопасность - свойство приписываемое объекту, надежно защищенному от опасных для него воздействий.**

Следовательно, понятие безопасности имеет две стороны:

* внешнюю, определяющую воздействие объекта на среду,
* внутреннюю, характеризующую свойства сопротивляемости объекта по отношению к действиям среды.

**Внутренняя безопасность** — характеристика целостности системы или показатель ее гомеостаза, описывает способность системы поддерживать свое нормальное функционирование в условиях внешних и внутренних воздействий.

**Внешняя безопасность** — способность системы взаимодействовать со средой без нарушения гомеостаза последней, воздействие системы на среду не приводит к необратимым изменениям или нарушениям важнейших параметров, характеризующих состояние среды, принятое за допустимое.

 **Безопасность — состояние развития защищенности жизненно важных интересов социума (личности, общества, государства) и его структур от внутренних и внешних угроз**.

Безопасность есть результат социальной деятельности по обеспечению безопасности личности, общества, государства. Деятельность по обеспечению безопасности личности, общества и государства возникает как социальный феномен в ходе разрешения противоречия между такой объективной реальностью, как опасность и потребность разумного существа, социального индивидуума, социальных групп и общностей предотвратить ее, локализовать, устранить последствия опасности.

**Объектом деятельности по обеспечению безопасности выступает опасность**. В этом случае **предметом** деятельности будут конкретные угрозы, опасности (военные, политические, экономические и пр.), а также конкретные материальные носители этих угроз (природные и социально-общественные явления и т.д.).

**Виды безопасности.**

Классификация категории «безопасность» может быть следующей.

**По признаку масштабности** в соответствии с видами опасности, пространственно-географическим взаимодействием социальных организмов принято различать следующие относительно самостоятельные геополитические уровни и виды безопасности:

* международная глобальная безопасность;
* международная региональная безопасность;
* национальная безопасность;
* местная безопасность.

**По признаку содержания угроз:**

* экологическая,
* Экономическая,
* Ресурсная,
* Информационная,
* Социальная,
* Научно-техническая,
* Энергетическая,
* Ядерная, политическая,
* Инновационная,
* правовая,
* культурная,
* техническая и др.

**По источнику угроз:**

* природная,
* техногенная.

В большинстве случаев при описании сложных явлений и при оценке опасности нескольких угроз используют:

* либо комбинированный термин (глобальная экологическая),
* либо национальная безопасность, которая характеризует степень защиты государства и включает в качестве основных элементов экол., экон., финансовой, инф. и др. виды безопасности.

**2. Понятие национальной безопасности. Компоненты и виды национальной безопасности.**

**Национальные интересы для любой страны** — это объективный фактор, обусловленный всей совокупностью ее жизненных потребностей.

Их содержание — свое у каждой страны — обусловливает, какой должна быть политика государства, чтобы его целостность и благополучие были надежно обеспечены и защищены, ее граждане жили в уважаемом во всем мире государстве, а руководство и внешнеполитические деятели выполняли свое призвание — представлять и отстаивать интересы во всех частях планеты.

В национальных интересах аккумулируется отношение нации ко всей совокупности общественно-политических институтов, материальных и духовных ценностей.

**Национальные интересы России** — это совокупность сбалансированных интересов личности, общества и государства в экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других сферах.

К числу коренных, основополагающих национальных интересов относятся: **территориальная целостность страны, государственное самоопределение и политическое самоуправление народа,** достойное место в мировом сообществе среди других подобных образований, процветание страны и населения на основе обеспечения прав личности и благополучия всех составляющих его социальных групп.

**Объекты национальной безопасности** - это реально существующие явления, процессы и отношения, защита которых составляет стратегическую цель и основное содержание безопасности.

Объектами национальной безопасности в соответствии с данным определением могут быть личность (человек), общество (народ), государство (нация), взаимоотношения между ними, а также явления и процессы, сопровождающие их взаимоотношения.

Объект национальной безопасности — это система «территория России — народы государства — уклад их жизни». Выбор вязан с тем, что она содержит не только нацию (народы России), но и ее базовые ценности, необходимые для обеспечения жизнедеятельности народов России и нации в целом.

**Национальные ценности — принадлежащая стране материальная, интеллектуальная и духовная собственность как основа ее существования и развития.**

**Национальный образ жизни — это исторически принятые отдельным национальным образованием или всем обществом в данной стране и наиболее распространенные и устойчивые формы социального и индивидуального поведения, нравственный уклад и система оценок, произвольные нарушения которых приводят к негативным социальным последствиям и (или) утрате самобытности.**

**Предмет национальной безопасности** — объективные закономерности появления и снижения ущерба, обусловленного антропогенно-социальными, природно-экологическими и техногенно-производственными угрозами и вызовами нации, ее базовым потребностям, ценностям и интересам.

Включает в себя «опасности, угрозы, вызовы, риски, ущерб».

**Опасность —** вполне осознаваемая, объективно существующая, но не фатальная вероятность (возможность) негативного воздействия на социальный организм или на что-либо, определяемая наличием объективных и субъективных факторов, обладающих поражающими свойствами, в результате которого может быть причинен какой-либо ущерб, вред, ухудшающий его состояние и/или условия жизнедеятельности и придающий его развитию нежелательные динамику (характер, темпы) или параметры (свойства, формы и т.д.).

**Ущерб** — результат разрушительного изменения целостности и/или свойств конкретных личностей (граждан) и принадлежащих им материальных или духовных ценностей.

**Понятие национальной безопасности** включает в себя в качестве основных элементов (видов) экономическую, социальную, экологическую, финансовую, ресурсную, ядерную, информационную безопасности интегрирует в себе ряд частных безопасностей и на их основе позволяет более полно оценивать степень защиты интересов государства от различных не только отдельных угроз, но и при их совместном воздействии.

Национальная безопасность в свою очередь подразделяется на:

* государственную безопасность;
* локальную (региональную) безопасность;
* частную (фирм и личности) безопасность.
* Различные аспекты национальной безопасности включают следующие понятия:
* национально-государственная безопасность;
* федеральная безопасность;
* общественная безопасность.

В зависимости от типов угрозы, а также в содержательном плане для международной и национальной безопасности выделяются следующие сферы (области) ее проявления и обеспечения:

* экологическая безопасность;
* экономическая безопасность;
* военная безопасность;
* ресурсная безопасность;
* информационная безопасность;
* социальная безопасность;
* научно-техническая безопасность;
* энергетическая безопасность;
* ядерная безопасность;
* политическая безопасность;
* инновационная безопасность;
* правовая безопасность;
* культурная безопасность;
* техническая безопасность и др.

В зависимости от источника угрозы при анализе катастроф, чрезвычайных ситуаций и аварий, а также ликвидации стихийных бедствий используют понятия:

* природная безопасность;
* техногенная безопасность.

**Национальная безопасность — защищенность жизненно важных интересов личностей (граждан), общества и государства, а также национальных ценностей и образа жизни от широкого спектра внешних и внутренних угроз, различных по своей природе (политических, военных, экономических, информационных, экологических и др.)**.

**Национальная безопасность — это состояние, при котором в государстве защищены национальные интересы страны в широком их понимании, включающем политические, социальные, экономические, военные, экологические аспекты, риски, связанные с внешнеэкономической деятельностью, распространением оружия массового поражения, а также предотвращения угрозы духовным и интеллектуальным ценностям народа .**

**Национальная безопасность — способность нации удовлетворять потребности, необходимые для ее самосохранения, самовоспроизводства и самосовершенствования с минимальным риском ущерба для базовых ценностей ее нынешнего и будущих поколений.**

В ряде случаев при описании сложных явлений и при оценке опасности нескольких угроз используют комбинированное название безопасности или вводят условное название. В качестве примера комбинированного названия безопасности можно привести широко применяемое понятие глобальной экологической безопасности, которое характеризует состояние защиты человечества от экологической угрозы.

Основное различие между национальной и государственной безопасностью в том, что нация создала государство и гибель нации приведет и к гибели России. Поэтому национальная безопасность приоритетнее для России, чем государственная безопасность.

**3. Основные элементы концепции национальной безопасности.**

**Сущность проблемы**

Безопасность Российской Федерации — одна из качественных характеристик конкретного исторического комплекса (социума), существующего в определенных пространственных, временных, географических условиях, составными элементами которого являются личность, общество и государство.

Концепция национальной безопасности Российской Федерации — система взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз во всех сферах жизнедеятельности. В Концепции сформулированы важнейшие направления государственной политики Российской Федерации.

 I. Россия в мировом сообществе

 II. Национальные интересы России

 III. Угрозы национальной безопасности Российской Федерации

 IV. Обеспечение национальной безопасности Российской Федерации

Исходя из положений концепции национальной безопасности, разрабатываются концепции (доктрины) внешнеполитической, экономической, общественной, оборонной, экологической, информационной и иных видов безопасности, включая охрану здоровья населения.

Программа действий по реализации положений концепции национальной безопасности на тот или иной конкретный промежуток времени называется стратегией обеспечения национальной безопасности.

**Под национальной безопасностью Российской Федерации понимается безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в Российской Федерации.**

Национальная безопасность России — это состояние или свойство государства обеспечивать адекватное реагирование в условиях постоянного дестабилизирующего воздействия военных, экономических политических, экологических, социальных, техногенных, информационных, демографических и психологических факторов. Эти меры должны быть направлены как на ликвидацию угроз и опасностей, так и на защиту интересов отдельного человека и государства в целом.

**Национальные интересы России**  — **это совокупность сбалансированных интересов личности, общества и государства в экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других сферах.** Они носят долгосрочный характер и определяют основные цели, стратегические и текущие задачи внутренней и внешней политики государства.

На каждом этапе развития государства определяются его национальные интересы. Для России в данный период таковыми являются:

1. Предотвращение угроз по всему их спектру - главный национальный интерес России.

2. Территориальная целостность государства. До настоящего времени реальной остается угроза единству России. Сепаратизм приобретает новые формы и из политического трансформируется в торгово-экономический со всеми вытекающими последствиями.

3. Сохранение гражданского мира, свободы и прав должно быть реализовано в законах и существующих государственных институтах России.

4. Интересы России в политической сфере. В определяющей мере они обусловлены ее геостратегическим положением.

**Долгосрочные** национальные интересы включают:

* сохранение общей стабильности в мире, способной противостоять локальным вооруженным конфликтам;
* ликвидацию очагов напряженности вблизи территории России;
* сохранение нормальных отношений со всеми государствами и перевод этих отношений на уровень партнерства;
* управление и развитие миротворческих возможностей ООН, ОБСЕ и других в целях скорейшего политического урегулирования конфликтов, угрожающих перерасти в вооруженное противостояние;
* дальнейшее углубление процесса реформирования Вооруженных Сил до современного уровня для обеспечения безопасности и выполнения международных обязательств РФ.

**Среднесрочные интересы** России заключаются в нормализации и стабилизации как внутреннего положения, так и обстановки в ближайшем окружении — странах СНГ, Афганистане, в других регионах, в том числе на Ближнем Востоке и в Азиатско-Тихоокеанском регионе.

**Краткосрочные** интересы России:

* прекращение межнациональных конфликтов в районах, прилегающих к кавказской границе России;
* достижение договоренности об экономическом пространстве в рамках бывшего СССР и, соответственно, режиме границ между государствами;
* претворение в жизнь договоренности, касающейся режима обеспечения государственных границ по всему периметру бывшего СССР;
* достижение договоренностей между Россией и другими государствами СНГ по вопросам защиты от ядерного нападения, а также по укреплению международного режима нераспространения ядерного оружия.
* Экономические интересы России:
* совершенствование концепции национальной экономической безопасности; это обусловлено тем, что сегодня политические и военные составляющие статуса России как великой державы опираются на недостаточно надежный экономический базис.
* продолжение развития исследований, практического освоения и рационального использования минеральных и живых ресурсов континентального шельфа и исключительной экономической зоны РФ, расположенных за пределами сухопутной и морской территории России;
* принятие энергичных законодательных мер, препятствующих разбазариванию ресурсов, принадлежащих всей РФ.

5. Национальные интересы России включают в себя прекращение межнациональных конфликтов и междоусобиц, защиту гражданских, прав, свобод, чести и достоинства россиян, обеспечение массированной политической, экономической и культурно-образовательной поддержки русских общин, автономий за рубежом.

6. Жизненно важные интересы России:

* обеспечение ее суверенитета и территориальной целостности;
* построение правового демократического государства на основе конституционного строя;
* экономическое возрождение страны и улучшение благосостояния ее народа;
* развитие международных отношений на основе верховенства закона, демократии, прав человека.

Национальные интересы России в **пограничной сфере** заключаются в создании политических, правовых, организационных и других условий для обеспечения надежной охраны государственной границы РФ, в соблюдении установленных законодательством РФ порядка и правил осуществления экономической и иных видов деятельности в пограничном пространстве РФ.

Национальные интересы России в **экологической сфере** заключаются в сохранении и оздоровлении окружающей среды.

Важнейшие составляющие национальных интересов России — защита личности, общества и государства от терроризма, в том числе международного, а также от чрезвычайных ситуаций природного и техногенного характера и их последствий, а в военное время — от опасностей, возникающих при ведении военных действий или вследствие этих действий.

Во **внутриполитической сфере** национальные интересы России состоят в сохранении стабильности конституционного строя, институтов государственной власти, в обеспечении гражданского мира и национального согласия, территориальной целостности, единства правового пространства, правопорядка и в завершении процесса становления демократического общества, в нейтрализации причин и условий, способствующих возникновению политического и религиозного экстремизма, этносепаратизма и их последствий — социальных, межэтнических и религиозных конфликтов, терроризма.

Национальные интересы России в **социальной сфере** заключаются в обеспечении высокого уровня жизни народа.

Национальные интересы в **духовной сфере** состоят в сохранении и укреплении нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Национальные интересы России в **международной сфере** заключаются в обеспечении суверенитета, упрочении позиций России как великой державы — одного из влиятельных центров многополярного мира, в развитии равноправных и взаимовыгодных отношений со всеми странами и интеграционными объединениями, прежде всего с государствами-участниками Содружества Независимых Государств и традиционными партнерами России, в повсеместном соблюдении прав и свобод человека и недопустимости применения при этом двойных стандартов.

Национальные интересы России в **информационной сфере** заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Национальные интересы России в **военной сфере** заключаются в защите ее независимости, суверенитета, государственной и территориальной целостности, в предотвращении военной агрессии против России и ее союзников, в обеспечении условий для мирного, демократического развития государства.

Усиливаются **угрозы национальной безопасности Российской Федерации в информационной сфере.** Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

**Современные угрозы и вызовы национальной безопасности России**

Угрозы национальной безопасности тесно связаны с национальными интересами государства, в том числе и за пределами его территории. В каждом конкретном случае для их ликвидации требуются особые формы и методы деятельности государства: применение соответствующих специальных органов, сил и средств государства.

Определение основных внешних и внутренних угроз и соответствующие им рекомендации по совершенствованию законодательства по национальной безопасности, касающиеся неотложных стратегических мер по самосохранению нации, могут быть получены только в результате полномасштабного анализа современной ситуации в России и в мире в целом. Игнорирование происходящих в мире перемен, наряду с ошибками во внешней и внутренней политике, привело Россию к концептуальной дезориентации.

Обеспечение национальной безопасности РФ включает в себя защиту культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, сохранение культурного достояния всех народов России, формирование государственной политики в области духовного и нравственного воспитания населения, введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие, эксплуатирующих низменные проявления, а также включает в себя противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

Духовное обновление общества невозможно без сохранения роли русского языка как фактора духовного единения народов многонациональной России и языка межгосударственного общения народов государств-участников СНГ.

В целях обеспечения сохранности и развития нашего культурного и духовного наследия необходимо создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры.

**Литературы**

1. Концепция национальной безопасности Российской Федерации, ут­вержденная Указом Президента Российской Федерации от 10.01.2000 № 24 // Собрание законодательства Российской Федерации. - 2000. -№2.-ст. 170
2. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
3. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
4. Анин Б.Ю. Защита компьютерной информации. Петербург, 2010. - 384с.
5. Галатенко В.А. Барсуков В.С., Водолазний В.В. Современные технологии безопасности. - М.: «Нолидж», 2009. - 496 с.
6. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
7. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
8. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

[www.consultant.ru](http://www.consultant.ru)

[www.intuit.ru](http://www.intuit.ru).

[www.garant.ru](http://www.garant.ru)

**Лекция № 3**

**Нормативная база в области информационной безопасности**

1. Общая характеристика нормативной базы в области информационной безопасности.
2. Концептуальные документы по вопросам информационной безопасности.
3. Законы Российской Федерации, регулирующие отношения в области информационной безопасности:
4. Подзаконные акты в области информационной безопасности (Указы Президента, постановления, приказы, распоряжения, правила, инструкции, положения Правительства Российской Федерации, федеральных органов исполнительной власти).
5. Государственные стандарты по защите информации.

**1. Общая характеристика нормативной базы в области информационной безопасности.**

В состав нормативной базы в области информационной безопасности в России включаются:

1. Концептуальные документы по вопросам информационной безопасности.
2. Законы Российской Федерации, регулирующие отношения в области информационной безопасности:

а) устанавливающие правила и процедуры обеспечения информационной безопасности;

б) устанавливающие ответственность в области обеспечения информационной безопасности.

1. Подзаконные акты в области информационной безопасности (Указы Президента, постановления, приказы, распоряжения, правила, инструкции, положения Правительства Российской Федерации, федеральных органов исполнительной власти).
2. Государственные стандарты по защите информации.

**2. Концептуальные документы по вопросам информационной безопасности.**

* Конституция РФ ст. 2,23, 24, 29, 55, 71
* Концепция национальной безопасности (версия 2000 года). Указ Президента РФ №1300 от 17.12.97 (в ред. №24 от 10.01. 2000)
* Доктрина информационной безопасности Российской Федерации (Указ Президента от 9.09.2000)
* Федеральная программа обеспечения защиты государственной тайны в Российской Федерации до 2009 года.

**3. Законы Российской Федерации, регулирующие отношения в области информационной безопасности:**

**Законы, устанавливающие правила и процедуры обеспечения информационной безопасности:**

**ЗАКОН «О ГОСУДАРСТВЕННОЙ ТАЙНЕ»** (в ред. Федеральных законов от 06.10.1997 N 131-ФЗ, от 30.06.2003 N 86-ФЗ, от 11.11.2003 N 153-ФЗ, от 29.06.2004 N 58-ФЗ, от 22.08.2004 N 122-ФЗ, с изм., внесенными Постановлением Конституционного Суда РФ от 27.03.1996 N 8-П, определениями Конституционного Суда РФ от 10.11.2002 N 293-О, от 10.11.2002 N 314-О) регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

**ФЕДЕРАЛЬНЫЙ ЗАКОН «О КОММЕРЧЕСКОЙ ТАЙНЕ»** (Принят 29.07.2004) регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну.

Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

**ЗАКОН «ОБ АВТОРСКОМ ПРАВЕ И СМЕЖНЫХ ПРАВАХ»** (9 июля 1993N 5351-1 в ред. Федеральных законов от 19.07.1995 N 110-ФЗ, от 20.07.2004 N 72-ФЗ) регулирует отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания (смежные права).

**ФЕДЕРАЛЬНЫЙ ЗАКОН «ОБ АРХИВНОМ ДЕЛЕ В РОССИЙСКОЙ ФЕДЕРАЦИИ»** (22 октября 2004 годаN 125-ФЗ ) регулирует отношения в сфере организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов независимо от их форм собственности, а также отношения в сфере управления архивным делом в Российской Федерации в интересах граждан, общества и государства.

**ФЕДЕРАЛЬНЫЙ ЗАКОН «О ТЕХНИЧЕСКОМ РЕГУЛИРОВАНИИ»** (27 декабря 2002 годаN 184-ФЗ Принят Государственной Думой 15 декабря 2002 года Одобрен Советом Федерации 18 декабря 2002 года) регулирует отношения, возникающие при:

* разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации;
* разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
* оценке соответствия.

Настоящий Федеральный закон также определяет права и обязанности участников регулируемых настоящим Федеральным законом отношений.

Требования к функционированию единой сети связи Российской Федерации и к продукции, связанные с обеспечением целостности, устойчивости функционирования указанной сети связи и ее безопасности, отношения, связанные с обеспечением целостности единой сети связи Российской Федерации и использованием радиочастотного спектра, соответственно устанавливаются и регулируются законодательством Российской Федерации в области связи.

Действие настоящего Федерального закона не распространяется на государственные образовательные стандарты, положения (стандарты) о бухгалтерском учете и правила (стандарты) аудиторской деятельности, стандарты эмиссии ценных бумаг и проспектов эмиссии ценных бумаг.

 **ФЕДЕРАЛЬНЫЙ ЗАКОН «О СВЯЗИ»** (7 июля 2003 года N 126-ФЗ
Принят Государственной Думой 18 июня 2003 года Одобрен Советом Федерации 25 июня 2003 года (в ред. Федеральных законов от 22.08.2004 N 122-ФЗ, от 02.11.2004 N 127-ФЗ, с изм., внесенными Федеральным законом от 23.12.2003 N 186-ФЗ) устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

**Законы, устанавливающие ответственность в области информационной безопасности.**

Вторая составляющая законодательства в области защиты информации – законодательство, устанавливающее ответственность за покушения на эти сведения.

**ГРАЖДАНСКИЙ КОДЕКС** **РФ** определяет правовое положение участников гражданского оборота, устанавливает обязательность документирования, виды и разновидности документов, создаваемых в целях фиксации актов гражданских взаимоотношений, регистрации фактов их возникновения или прекращения, подтверждения правоотношений, требования к форме и содержанию документов и др.

 **КОДЕКС ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ** предусматривает ответственность за несоблюдение правил хранения, комплектования, учета и использования архивных документов

**УГОЛОВНЫЙ КОДЕКС РФ** предусматривает ответственность за контрабанду, утрату документов, содержащих государственную тайну, похищение или повреждение документов, имеющих особую историческую, научную, художественную и культурную ценность, за приобретение или сбыт официальных документов, штампов, печатей

**ТРУДОВОЙ КОДЕКС РФ (2002)** устанавливает обязательность применения каждой организацией независимо от ее организационно-правовой формы ряда локальных правовых актов (коллективный договор, соглашение, правила внутреннего трудового распорядка, положение об использовании и защите персональных данных и др.), называет документы, которыми документируется прием, перевод, увольнение, командирование, отпуска, поощрения и взыскания работников, определяет структуру текста и порядок оформления некоторых из них, устанавливает сроки подготовки документов, определяет порядок защиты персональных данных и др.

**Литература:**

1. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

 **Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.garant.ru](http://www.garant.ru)

**Лекция № 4**

**Сущность и понятие защиты информации**

1. Значение раскрытия сущности и определения понятия защиты информации. Существующие подходы к содержательной части понятия защиты информации.

2. Методологическая основа для раскрытия сущности и определения понятия защиты информации – понятие «защита».

3. Понятие уязвимости информации и ее форм и видов.

4. Определение защиты информации.

5. Понятие безопасности информации.

**1. Значение раскрытия сущности и определения понятия защиты информации.**

**Существующие подходы к содержательной части понятия защиты информации.**

По **содержательной части** защита информации рассматривается как: предупреждение несанкционированного доступа к информации; создание условий, ограничивающих распространение информации; ограждение права собственника на владение и распоряжение информацией; предотвращение утечки, хищения, утраты, несанкционированного уничтожения, копирования, модификации, искажения, блокирования, разглашения информации, несанкционированных и непреднамеренных воздействий на нее; сохранение полноты, надежности, целостности, достоверности, конфиденциальности информации и т.д.

**Способом реализации** содержательной части понятия одни авторы называют совокупность мероприятий, методов и средств, другие -деятельность, у третьих он вообще отсутствует.

**2. Методологическая основа для раскрытия сущности и определения понятия защиты информации – понятие «защита».**

Методологической основой для раскрытия сущности и определения понятия защиты информации должно быть определение понятия **защита** в целом, безотносительно к предмету защиты.

В толковых словарях термин защита интерпретируется двояко: как процесс охраны, сбережения, спасения от кого, чего-нибудь неприятного, враждебного, опасного и как совокупность методов, средств и мер, принимаемых для предотвращения, предупреждения чего-то. Таким образом, **содержательная часть** в этих определениях по смыслу совпадает - **это предотвращение, предупреждение чего-то опасного, враждебного.** Если соотнести это положение с защитой информации, то самым опасным для собственника информации является **нарушение установленного статуса информации,** и поэтому содержательной частью защиты должно быть предотвращение такого нарушения.

**Нарушение статуса любой информации заключается в нарушении ее физической сохранности вообще либо у данного собственника (в полном или частичном объеме), структурной целостности, доступности для правомочных пользователей.** Нарушение статуса конфиденциальной информации, в том числе составляющей государственную тайну, дополнительно включает в себя нарушение ее конфиденциальности (закрытости для посторонних лиц).

**3. Понятие уязвимости информации и ее форм и видов.**

Нарушение статуса информации обусловлено ее у**язвимостью, которая означает неспособность информации самостоятельно противостоять дестабилизирующим воздействиям, сохранять при таких воздействиях свой статус.**

**Формы уязвимости**

Но уязвимость информации - понятие собирательное, она не существует вообще, а проявляется (выражается) в различных **формах.** В научной литературе и нормативных документах не сформировался термин форма проявления уязвимости ин­формации, но самих конкретных форм называется множество. При этом значительное количество перечисляемых форм являются синонимами или разновидностями одних и тех же явлений, некоторые не могут быть отнесены к формам по своей сущности.

**К формам проявления уязвимости информации, выражающим результаты дестабилизирующего воздействия на информацию, должны быть отнесены:**

1. хищение носителя информации или отобра­женной в нем информации (кража); (Хищение информации часто ставится в один ряд с ее **несанкционированным копированием, размножением, съемом, перехватом.** Однако пос­ледние являются не формами проявления уязви­мости информации, а **способами хищения)**,
2. потеря носителя информации (утеря);
3. несанкционированное уничтожение носителя информации или отображенной в нем информации (разрушение);
4. искажение информации (несанкционированное изменение, несанкционированная модификация, подделка, фальсификация); Термины модификация, подделка, фальсифи­кация не совсем адекватны термину искажение, они имеют нюансы, но суть их одна и та же - не­санкционированное частичное или полное изменение первоначальной информации.
5. блокирование информации;
6. разглашение информации (несанкционированное распространение, раскрытие).

Та или другая форма уязвимости информации может реализоваться при преднамеренном или случайном, непосредственном или опосредованном дестабилизирующем воздействии различны­ми способами на носитель информации или саму информацию со стороны определенных источников воздействия.

**Виды уязвимости - утрата и утечка.**

Но результатами проявления форм уязвимости информации могут быть либо утрата, либо утечка информации, либо одновременно то и другое.

К **утрате** как конфиденциальной, так и защищаемой части открытой информации приводят хищение и потеря носителей информации, несанкционированное уничтожение носителей информации или только отображенной в них информации, искажение и блокирование информации. Утрата может быть полной или частичной, безвозвратной или временной (при блокировании информации), но в любом случае она наносит ущерб собственнику информации.

Термин **утечка** информации, вероятно, не самый благозвучный, однако он более емко, чем другие термины, отражает суть явления, к тому же он давно уже закрепился в научной литературе и нормативных документах. Правда, единого подхода к определению этого термина нет. Наиболее распространенные определения утечки в обобщенном виде сводятся:

1.Либо к неправомерному (неконтролируемому) выходу конфиденциальной информации за пределы организаций и круга лиц, которым эта информация доверена,

2. Либо к несанкционированному завладению конфиденциальной информацией соперником. При этот термин конфиденциальная информация иногда неправомерно заменяется термином защищаемая информация.

**Первый вариант** не раскрывает в полной мере сущности утечки, поскольку он не принимает во внимание последствий неправомерного выхода конфиденциальной информации. А они могут быть двоякими: или информация попала в руки лиц, не имеющих к ней санкционированного доступа, или не попала. Например, потерянный носитель конфиденциальной информации означает неправомерный выход информации за пределы лиц, имеющих к ней доступ, но он может попасть в чужие руки, а может быть и прихвачен мусороуборочной машиной и уничтожен в установленном для мусора порядке. В последнем случае **утечки информации не происходит**.

**Второй вариант** утечку информации связывает с неправомерным завладением конфиденциальной информацией только соперником. В таком варианте, к примеру, средства массовой информации, которым нередко поставляют или они сами добывают конфиденциальную информацию, должны рассматриваться в качестве соперников собственника информации, в этом случае настоящий соперник получает информацию правомерно, через СМИ.

**Утечка информации - неправомерный выход конфиденциальной информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, результатом которого является получение информации лицами, не имеющими к ней санкционированного доступа.**

**Соотношение понятий утечка, разглашение, распространение, передача информации.**

Термин утечка информации нередко, в том числе и в нормативных документах, заменяется или отождествляется с терминами разглашение информации, распространение информации и даже передача информации. Такой подход представляется неправомерным.

Термин **разглашение информации** означает несанкционированное доведение конфиденциальной информации до потребителей, не имеющих права доступа к ней, таким образом, он предполагает, что разглашение исходит от кого-то, осуществляется кем-то. Результатом разглашения является утечка информации, но утечка не сводится только к разглашению. Утеска – результат разглашения.

**Термин распространение** применительно к конфиденциальной информации без слов несанкционированное или необоснованное ничего не выражает, поскольку распространение информации может быть и обоснованным, к тому же он опять-таки предполагает, что информация исходит от кого-то.

**Термин передача** информации говорит сам за себя.

Помимо разглашения, утечка может произойти и в результате потери и хищения носителя конфиденциальной информации, а также хищения отображенной в носителе информации при сохранности носителя у собственника (владельца). Может произойти - не означает, что произойдет. Выше уже отмечалось, что потеря носителя не всегда приводит к утечке информации. Хищение конфиденциальной информации также не всегда связано с получением ее лицами, не имеющими к ней доступа. Имелось немало случаев, когда хищение носителей конфиденциальной информации осуществлялось у коллег по работе допущенными к этой информации лицами с целью подсидки, причинения вреда коллеге. Такие носители, как правило, уничтожались лицами, похитившими их. Но в любом случае потеря и хищение если и не приводят к утечке информации, то создают угрозу утечки.

Поэтому можно сказать, что **к утечке конфиденциальной информации приводит ее разглашение и могут привести хищение и потеря**. Сложность состоит в том, что зачастую невозможно определить:

* во-первых, сам факт разглашения или хищения информации при сохранности носителя информации у собственника (владельца),
* во-вторых, попала ли информация вследствие ее хищения или потери посторонним лицам.

При этом не следует отождествлять хищение с разглашением, как это иногда делается. Хищение может привести и часто приводит к разглашению и в последнем случае выступает в роли опосредованного способа разглашения, но, во-первых, результатом хищения не всегда бы­вает разглашение, во-вторых, разглашение конфи­денциальной информации осуществляется не только посредством ее хищения.

Утрата и утечка информации могут рассматриваться как виды уязвимости информации.

**4. Определение защиты информации.**

Вторая составляющая сущности защиты ин­формации - способ реализации содержательной части - в толковых словарях, как уже отмечалось, представлена как процесс или как совокупность методов, средств и мероприятий.

Защита информации включает в себя определенный набор методов, средств и мероприятий, однако ограничивать способ реализации только этим было бы неверно. Защита информации должна быть системной, а в систему помимо методов, средств и мероприятий входят и другие компоненты: объекты защиты, органы защиты, пользователи информации. При этом защита не должна представлять собой нечто статичное, а являться непрерывным процессом. Но этот процесс не осуществляется сам по себе, а происходит в результате деятельности людей. Деятельность же, по определению, включает в себя не только процесс, но и цели, средства и результат. Защита информации не может быть бесцельной, безрезультатной и осуществляться без помощи определенных средств. Поэтому именно деятельность и должна быть способом реализации содержательной части защиты.

Объединив содержательную часть защиты информации и способ реализации содержательной части, можно сформулировать следующее определение:

**Защита информации - деятельность по предотвращению утраты и утечки конфиденциальной информации и утраты защищаемой открытой информации.**

Учитывая, что определение должно быть лаконичным, а термин утрата и утечка защищаемой информации поглощает все формы проявления уязвимости конфиденциальной и защищаемой части открытой информации, можно ограничиться более кратким определением при условии дифференцированного его преломления в практической работе: **Защита информации - деятельность по предотвращению утраты и утечки защищаемой информации.**

**5. Понятие безопасности информации.**

С понятием защиты информации тесно связано понятие безопасности информации.

Термин безопасность информации имеет двойное смысловое значение, его можно толковать:

1. и как безопасность самой информации,

При этом безопасность самой информации не вписывается в однозначное понимание. С одной стороны, это может означать безопасность информации с точки зрения изначальной **полноты и надежности информации (т.е. безопасность с точки зрения содержания)**, с другой стороны, — **защищенность установленного статус-кво информации (безопасность с точки зрения формы информации).**

1. и как отсутствие угроз со стороны информации субъектам информационных отношений.

В нормативных документах и литературе безопасность информации рассматривается только в разрезе ее защищенности, и это, вероятно, оправдано при наличии термина информационная безопасность.

Существует несколько определений понятия **безопасность информации**. Общий подход: **безопасность информации** **как состоянию защищенности (или защиты) информации.** Это не вызывает возражений, ибо сам термин безопасность означает отсутствие опасностей, что определенным образом корреспондируется с термином состояние защищенности.

 **Но** определения существенно различаются между собой содержательной частью - защищенности от чего. Сюда относят:

* от внутренних и внешних угроз; (непонятно)
* от утеч­ки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (поддел­ки), несанкционированного копирования, блоки­рования информации и т.п.; (перепутаны виды и формы уязвимости)
* от случайных или преднамеренных несанкционированных воздействий на информацию или несанкционированного ее получения;
* от случайного или преднамеренного доступа лиц, не имеющих права на получение ин­формации, ее раскрытие, модификацию или раз­рушение, и др.

**Т.о., Безопасность информации – это состояние защищенности информации от воздействий, нарушающих ее статус.**

Из определений понятий защита информации и безопасность информации вытекает и **соотношение** между ними: защита информации направлена на обеспечение безопасности информации или, другими словами, безопасность информации обеспечивается с помощью ее защиты (безопасность информации – результат ее защиты).

**Литература:**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. Анин Б.Ю. Защита компьютерной информации. Петербург, 2010. - 384с.
4. Галатенко В.А. Барсуков В.С., Водолазний В.В. Современные технологии безопасности. - М.: «Нолидж», 2009. - 496 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
7. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

 **Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция № 5**

**Организационные основы и методологические принципы**

**защиты информации**

1. Состав и структура системы обеспечения информационной безопасности Российской Федерации (СОИБ РФ).

2. Основные элементы организационной основы СОИБ РФ.

3. Силы обеспечения ИБ РФ.

4. Методологические принципы защиты информации.

**7.1. Состав и структура системы обеспечения информационной безопасности Российской Федерации (СОИБ РФ).**

В Доктрине информационной безопасности РФ определены организационная основа системы обеспечения информационной безопасности РФ (СОИБ РФ) и основные функции этой системы. Однако состава и структуры СОИБ РФ Доктрина не определяет. В ней сделана лишь ссылка на то, что в рамках этой системы созданы и функционируют самостоятельные системы, такие как система защиты государственной тайны и государственная система защиты информации.

 **Система обеспечения информационной безопасности** – совокупность органов, методов (способов), сил и средств обеспечения информационной безопасности.

Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере и является частью системы обеспечения национальной безопасности страны.

Она строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов РФ.

Состав СОИБ РФ представлен на рис. 1.

СИСТЕМЫ И ПОДСИСТЕМЫ

# С О И Б

# РФ

Органы управления и обеспечения

ИБ РФ

Силы

обеспечения

ИБ РФ

Методы

обеспечения

ИБ РФ

Средства

обеспечения

ИБ РФ

Система лицензирования деятельности в области защиты государственной тайны

Система лицензирования деятельности в области защиты конфиденциальной информации

Система лицензирования деятельности в области криптографической защиты информации

Система

сертификации средств защиты информации

Система сертификации криптографических средств защиты информации

Система защиты государствен-ной тайны

Государственная система защиты информации в РФ от технической разведки и утечки по техническим каналам

Другие системы и

Другие системы и подсистемы

Система защиты правительственной связи и информации

**2. Основные элементы организационной основы СОИБ РФ.**

**Органы управления и обеспечения ИБ РФ** составляют организационную основу СОИБ РФ. Основные элементы организационной основы СОИБ РФ приведены на рис.2.

**Президент**  РФ руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности; санкционирует действия по обеспечению информационной безопасности РФ; в соответствии с законодательством РФ формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению ИБ РФ; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения ИБ РФ , а также меры по реализации Доктрины ИБ РФ.

 **Палаты** Федерального Собрания РФ на основе Конституции РФ по представлению Президента и Правительства РФ формируют законодательную

**Основные элементы организационной основы системы обеспечения информационной безопасности РФ**

Совет

 Федерации

Президент РФ

Государственная Дума

Правительство РФ

#### Совет

Безопасности РФ

Федеральные органы исполнительной власти

Органы судебной власти

Граждане РФ

Общественные объединения

Межведомственные

и государственные комиссии

создаваемые Президентом и

Правительством РФ

Органы

местного самоуправления

Органы исполнительной власти

субъектов РФ

Рис.2 Основные элементы организационной основы СОИБ РФ

 **Правительство** **РФ,** в пределах своих полномочий, и с учетом сформулированных в ежегодных посланиях Президента РФ Федеральному Собранию приоритетных направлений в области обеспечения ИБ РФ, координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ. Также, при формировании в установленном порядке проектов федерального бюджета на соответствующие годы, предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

 **Совет**  **Безопасности РФ** проводит работу по выявлению и оценке угроз информационной безопасности РФ, оперативно подготавливает проекты решений Президента по предотвращению таких угроз, разрабатывает предложения в области обеспечения ИБ РФ, а также предложения по уточнению отдельных положений Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов РФ решений Президента в этой области.

 **Федеральные** **органы исполнительной власти** обеспечивают исполнение законодательства РФ, решений Президента и Правительства в пределах своей компетенции, разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту и в Правительство

 **Межведомственные и государственные комиссии**, создаваемые Президентом и Правительством РФ, решают в соответствии с предоставленными им полномочиями задачи обеспечения ИБ РФ.

 **Органы исполнительной власти субъектов РФ**, взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства РФ, решений Президента и Правительства в области обеспечения ИБ РФ, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения ИБ РФ; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения ИБ РФ.

**Органы местного самоуправления** обеспечивают соблюдение законодательства РФ в области обеспечения информационной безопасности России.

 **Органы судебной власти** осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности РФ.

**3. Силы обеспечения информационной безопасности РФ.**

Основу сил обеспечения информационной безопасности РФ составляют органы исполнительной власти, в задачи которых, в соответствии с законодательством, входит деятельность по обеспечению информационной безопасности. Для этого эти органы имеют соответствующие части, подразделения и службы. К ним относятся:

* Федеральная служба безопасности РФ (ФСБ);
* Служба внешней разведки РФ (СВР)
* **Федеральная служба по техническому и экспортному контролю** (БывшаяГосударственная техническая комиссия при Президенте РФ;
* Министерство внутренних дел РФ (МВД);
* Органы судебной власти;
* Федеральная таможенная служба РФ;
* Федеральная служба по техническому регулированию и метрологии РФ.

**Функции ФСБ по защите информации:**

- участвует в разработке и реализации мер по обеспечению информационной безопасности страны, по защите сведений, составляющих государственную тайну, в **лицензировании** деятельности предприятий, учреждений и организаций, связанной с использованием сведений, составляющих государственную тайну, оказанием услуг по защите государственной тайны; определяет основные направления деятельности органов федеральной службы безопасности в этих областях;

- осуществляет контроль за обеспечением защиты сведений, составляющих государственную тайну, в государственных органах, воинских формированиях, на предприятиях, в учреждениях и организациях; в установленном порядке осуществляет мероприятия, связанные с допуском граждан к сведениям, составляющим государственную тайну, а также с приемом на военную службу (работу) в органы ФСБ;

* организует и осуществляет шифровальные работы в ФСБ, а также контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов, воинских формирований, предприятий, учреждений и организаций (за исключением учреждений РФ, находящихся за ее пределами)и другие функции определённые в Положении о Федеральной службе безопасности Российской Федерации (утв. Указом Президента РФ от 6 июля 1998 г. N 806).

**ФСБ выполняет также функции, выполняемые ранее федеральными органами правительственной связи и информации (ФАПСИ).**

* организация и обеспечение эксплуатации, безопасности, развития и совершенствования правительственной связи, иных видов специальной связи и систем специальной информации для государственных органов;
* обеспечение в пределах своей компетенции сохранности государственных секретов; организация и обеспечение криптографической и инженерно-технической безопасности шифрованной связи в Российской Федерации и ее учреждениях за рубежом;
* лицензирование деятельности в области криптографической защиты информации и сертификация криптографических средств защиты;

**СВР РФ выполняет те же функции в этой области за рубежом.**

**Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ)** является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению технической защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную или служебную тайнуа также единую государственную научно-техническую политику в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

ФСТЭК организует деятельность государственной системы защиты информации в РФ от технических разведок и от ее утечки по техническим каналам.

ФСТЭК и региональные центры входят в состав государственных органов обеспечения безопасности Российской Федерации.

 В соответствии со своими функциями она осуществляет:

- координацию деятельности органов и организаций в области защиты информации, обрабатываемой техническими средствами;

- организационно-методическое руководство деятельностью по защите информации в КС;

- разработку и финансирование научно-технических программ по защите информации;

- утверждение нормативно-технической документации;

-функции государственного органа по сертификации продукции по требованиям безопасности информации;

- лицензирование деятельности предприятий по оказанию услуг в области защиты информации.

**Федеральная Служба по техническому регулированию и метрологии**  разрабатывает стандарты в области защиты информации.

**Органы МВД** ведут борьбу с правонарушителями в информационной сфере и компьютерными преступлениями. Для этого в структуре МВД создано специальное управление "К" для предотвращения и раскрытия компьютерных преступлений, преступлений связанных с нарушением авторских прав в сфере высоких технологий.

**Федеральная таможенная служба**  обязана предупреждать незаконный ввоз и вывоз из России "пиратской" продукции, обеспечивая тем самым защиту авторских и патентных прав.

**4. Методологические принципы защиты информации.**

**Принципы защиты информации** – это основополагающие идеи, важнейшие рекомендации по организа­ции и осуществлению этой деятельности на различных этапах ре­шения задач сохранения секретов. Они учитываются при созда­нии нормативной базы защиты информации, и даже более — за­кладываются в качестве норм в законах и подзаконных актах и, следовательно, приобретают обязательный для исполнителей ха­рактер.

Эти принципы выработаны длительной практикой организа­ции работ по защите информации в нашей стране, с учетом меж­дународного опыта.

Принципы защиты информации можно разделить на три груп­пы: правовые, организационные и используемые при защите ин­формации от ТСР и в средствах вычислительной техники (СВТ).

 **ПРАВОВЫЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ**

**1. Принцип законности**. В рамках долженствующего существова­ния правового государства деятельность предприятий и организаций всех форм собственности, всех должност­ных лиц и граждан должна осуществляться в рамках действующих законов.

Принцип законности в области защиты информации выража­ется прежде всего в том, что необходимо нормативно-правовое регулирование этой важной области общественных отношений в государстве. Законодательно должны быть:

* обозначены права раз­личных субъектов в области защиты информации, на засекречи­вание информации и установление правил ее защиты;
* определе­но, что является государственной, коммерческой, иной охраняе­мой законом тайной;
* установлена уголовная, административная, материальная, моральная ответственность за незаконное покуше­ние на защищаемую информацию и разглашение или передачу такой информации кому-либо, вследствие чего наступили или могли наступить вредные последствия для собственника (владель­ца) информации.

С другой стороны, должностные лица и другие работники пред­приятий и учреждений, которым по службе или работе доверяются секреты, в соответствии с действующими законами и подзаконны­ми актами, должны наделяться правами, позволяющими им ус­пешно осуществлять защиту доверенной им конфиденциальной или секретной информации, и на них должны налагаться обязанности по соблюдению соответствующего установленного режима, выполнение которого обеспечивает сохранность информации.

**2. Принцип приоритета международного права над внутригосу­дарственным.** Россия как преемница взятых бывшим Советским Союзом на себя обязательств признает также принцип приоритета международного права над внутренним. В частности, наша страна взяла на Венской встрече обязательство привести свое внутреннее законодательство в соответствие с положениями международных конвенций и соглашений, участником которых она является. От­сюда вытекает, что объектом засекречивания не могут быть сведе­ния, которые наше государство обнародует или сообщает согласно конвенциям и соглашениям, так как оно становится членом миро­вого экономического сообщества, вступило в МВФ и другие меж­дународные экономические организации. Одним из условий член­ства в этих организациях является предоставление информации о реальном положении дел в национальной экономике.

Это не исключает того, что РФ как суверенное государство может и должно засекречивать и защищать информацию, относя­щуюся к тем областям его деятельности, которые обеспечивают его национальную безопасность. Каждое государство имеет право само решать, что оно будет засекречивать, а что открывать. Одна­ко взаимность и равенство на национальные секреты между госу­дарствами или коалициями государств будет способствовать раз­витию взаимного доверия.

**3. Принцип одинаковой секретности** будет способствовать ук­реплению мер доверия в международных отношениях, помогать устранению асимметрии режимных ограничений, сложившихся в различных странах. Излишнее стремление по сокрытию инфор­мации от другой стороны всегда вызывает подозрение, так как такие действия обычно связывают с недобрыми намерениями одной стороны по отношению к другой.

**4. Принцип собственности и экономической целесообразности.**

Радикальные перемены, происходящие в российском общест­ве, не могли не затронуть лежащие в основе экономической ре­формы отношений по поводу собственности. Был принят ряд за­конов, регламентирующих сферу имущественных отношений, от­ношений собственности, в том числе относящихся к регулирова­нию прав на интеллектуальную собственность, на владение и рас­поряжение информацией, на защиту информации.

Это дало собственникам информации, объектов интеллекту­альной собственности право принимать меры к их защите с по­мощью различных правовых механизмов, в том числе с помощью патентов, норм авторского права, коммерческой тайны. Лишь собственник (владелец) информации имеет право определять, какую информацию следует засекретить и до какой степени и за­щищать как государственную или коммерческую тайну, или же запатентовать и защищать с помощью патента и оплачивать дея­тельность по защите любой охраняемой информации.

Секретность должна оцениваться как потребительское свойст­во и ее стоимость должна включаться в цену производимого про­дукта, за счет которой владельцем и будут осуществляться меро­приятия, обеспечивающие режим секретности. Секретность должна быть экономической категорией, и ее соблюдение в усло­виях рыночной экономики — дело владельцев секретов, промыш­ленной или банковской тайны, которые сами должны оценивать степень и время действия секретности с учетом полученной или упущенной выгоды. В области защиты государственной тайны действуют и другие (политические, военные и т.д.) факторы при решении проблем защиты информации.

**ОРГАНИЗАЦИОННЫЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ**

Организационные принципы претерпели за последние годы значительно меньше изменений, по сравнению с правовыми. Это объясняется тем, что они отражают общие по своей сути правила, подходы к защите секретов. Они используются и «работают» при любой общественно-политической и экономической системе и при защите любого вида охраняемой информации: государствен­ной или коммерческой тайны.

**1. Научный подход к организации защиты информации.**

Функционирующая в нашей стране общегосударственная сис­тема защиты информации создана с учетом имеющихся объемов защищаемой информации и используемых для ее обработки средств, традиций и опыта в области защиты государственных секретов, накопленных в предыдущие десятилетия. Создание такой системы потребовало научного осмысления таких проблем, как:

* разграничение компетенции в области защиты государствен­ной тайны по всей иерархической лестнице многочисленных ор­ганов и организаций и защиты коммерческой тайны;
* научное и законодательное определение понятий «государственная» и «ком­мерческая тайна», «служебная тайна», «персональные данные» и т.д.;
* разработка научных критериев определе­ния степени секретности информации и т.д.

В научных исследованиях проблем защиты информации используются **научные методы. Так, комплексный и системный подход** к организации защиты ин­формации предполагает:

* **с одной стороны**, выявление и анализ возможных каналов утечки защищаемой информации с учетом объемов такой информации и носителей, на которых она накап­ливается, и ее важности;
* **с другой стороны,** изучаются и анализи­руются возможности конкурента по собиранию и добыванию за­щищаемой информации не вообще, а в каждом конкретном слу­чае в отношении определенного предприятия, учреждения, отрас­ли или проблемы.

**Системный подход** позволяет создать органически взаимосвя­занную совокупность сил, средств и специальных методов по оп­тимальному ограничению сферы обращения засекреченной ин­формации, предупреждению ее утечки.

При создании системы защиты информации и осуществлении мероприятий по защите секретов от разглашения или новейших ТСР важно предусматривать разносторонние комплексные за­щитные меры, направленные на предупреждение утечки инфор­мации из сферы ее обращения.

**2. Максимальное ограничение числа лиц, допускаемых к защи­щаемой информации.**

Основной смысл этого принципа сводится к тому, что сохран­ность засекреченной информации находится в зависимости от ко­личества лиц, допущенных к обращению с нею. Чем уже этот круг, тем выше вероятность сохранения в тайне данной информа­ции. Организационно этот принцип решается следующим обра­зом: к секретным работам допускаются лица, имеющие, во-пер­вых, на то соответствующее разрешение в виде допуска, и во-вто­рых, из числа лиц имеющих допуск, — получившие разрешение на работу с конкретной информацией в виде доступа, который полу­чают только те, кто непосредственно связан по работе с этой ин­формацией.

Своеобразным проявлением этого принципа возможно также дробление технологической цепочки производства какого-либо изделия, продукта на отдельные операции, знание одной из кото­рых не дает возможность восстановить всю технологию. Каждая из операций засекречивается самостоятельно и переход специа­листа с одной операции на другую или вообще бывает невозмо­жен, или требует специального допуска и, следовательно, рас­смотрения вопроса — с какой целью это делается, если происхо­дит по инициативе работника.

**3. Персональная ответственность за сохранность доверенных секретов.** Этот принцип хорошо «работает», если каждый сотруд­ник, допущенный к защищаемой информации, понимает и осоз­нает, что сохранение в тайне этой информации и в его собствен­ных интересах. Если же работник видит, что сохранение какой-то информации в тайне нужно лишь предприятию или государству, а ему лично ничего не дает, то он к этому будет и относиться формально. Над ним будет тяготеть лишь груз боязни ответствен­ности.

Важным фактором, повышающим ответственность сотрудни­ков за сохранение доверенных им секретов, является обучение правилам защиты засекреченной информации и правилам обра­щения с конфиденциальными документами.

**4. Единство в решении производственных, коммерческих, фи­нансовых и режимных вопросов.** В этом принципе заложено одно из проявлений комплексного подхода к организации защиты ин­формации, имеющего, однако, относительно самостоятельное значение. Знание и учет этого принципа заключается в том, что лица, принимающие решения о засекречивании информации, бо­леющие больше, конечно, за решение производственных, финансовых, маркетинговых и иных подобных задач, не должны забы­вать и упускать из вида необходимость одновременного решения и режимных вопросов, там, где это необходимо.

**5. Непрерывность защиты информации.** Данный принцип за­ключается в том, что защита секретной или конфиденциальной информации должна начинаться с момента ее появления (полу­чения, создания, генерирования) на всех этапах ее обработки, передачи, использования и хранения, вплоть до этапа ее уничто­жения или рассекречивания.

**ПРИНЦИПЫ, ИСПОЛЬЗУЕМЫЕ ПРИ ЗАЩИТЕ ИНФОРМАЦИИ ОТ ТЕХНИЧЕСКИХ СРЕДСТВ РАЗВЕДКИ**

В организации деятельности по защите информации от технических средств разведки (ТСР) и в средствах вычислительной техники (СВТ) руководствуются, прежде всего, теми **же организационными и правовыми принципами,** о которых говорилось выше. Это объ­ясняется тем, что эти принципы имеют достаточно общий и уни­версальный характер. Эти принципы «работают» независимо от того, где, когда и кем осуществляется защита информации.

Однако имеются и **специфические принципы,** обусловленные особенностями предмета защиты, то есть носителей, на которых отображена защищаемая информация, используемых при этом силах, средствах и методах, а также учитываются средства и мето­ды добывания защищаемой информации соперником с помощью ТСР.

1. **Принципы защиты информации, используемые при организа­ции противодействия ТСР:**
* активность защиты информации — выражается в целена­правленном навязывании технической разведке ложного пред­ставления об объекте его разведывательных устремлений, в соот­ветствии с замыслом защиты;
* убедительность защиты информации — состоит в оправдан­ности замысла защиты условиям обстановки в соответствии с ха­рактером защищаемого объекта или свойствам окружающей среды, в применении технических решений защиты, соответствующих климатическим, сезонным и другим условиям;
* непрерывность защиты информации предполагает органи­зацию защиты объекта на всех стадиях его жизненного цикла:
предпроектном, проектном, в период разработки, изготовления
(строительства), испытания, эксплуатации и утилизации;
* разнообразие защиты информации — предусматривает исключение шаблона, повторяемости в выборе объекта прикрытия и путей еализации смысла защиты, в том числе с применением типовых решений.
1. **Принципы защиты информации, используемые в СВТ.** Основ­ными принципами защиты информации, имеющими специфи­ческий характер и используемыми в организации защиты инфор­мации в СВТ, являются, по мнению А.А.Шиверского, следующие:
* введе­ние избыточности элементов системы,
* резервирование элементов системы,
* защитные преобразования данных,
* контроль состояния элементов системы, их работоспособности и правильности функ­ционирования.

**Под введением избыточности элементов системы** понимается включение дополнительных компонентов сверх того минимума, который необходим для выполнения им всего множества своих функций. Избыточные элементы функционируют одновременно с основными, что позволяет создавать системы, устойчивые отно­сительно внешних и внутренних дестабилизирующих факторов и воздействий. Различают избыточность организационную, аппа­ратную, программно-алгоритмическую, информационную, и др.

**Защитные преобразования данных**, **контроль состояния эле­ментов системы, их работоспособности и правильности функци­онирования** будут рассмотрены нами ниже.

**Резервируются** обычно не все элементы системы защиты ин­формации, а особо важных компьютерных подсистем, чтобы в случае возникновения каких-то чрезвычайных обстоятельств, их можно было использовать для решения стоящих перед системой задач.

**Литература:**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. Анин Б.Ю. Защита компьютерной информации. Петербург, 2010. - 384с.
4. Галатенко В.А. Барсуков В.С., Водолазний В.В. Современные технологии безопасности. - М.: «Нолидж», 2009. - 496 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
7. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция № 7**

**Критерии, условия и принципы отнесения информации к защищаемой**

1. Понятие «тайна», ее признаки и виды.

2. Понятие «защищаемая информация» и его соотношение с понятием тайны.

3. Критерии отнесения открытой информации к защищаемой.

4. Критерии отнесения конфиденциальной информации к защищаемой.

5. Условия отнесения информации к защищаемой.

**1. Понятие «тайна», ее признаки и виды.**

Тайна — это понятие, имеющее несколько смысловых значе­ний.

1. В общем понимании тайна трактуется как нечто неразгадан­ное, еще непознанное. Употребляются, к примеру, такие выраже­ния, как «тайны природы», «тайны вселенной» и т.п., при этом подразумеваются те явления, сущность которых человеческий разум пока не постиг. Тайна рассматривается как **объективная категория** — как тайна природы. К этому виду тайн относятся непознанные явления, законы природы, мышления, общества.

2. Применительно к органам государственной власти и управле­ния под тайной понимается то, что скрывается от других, что из­вестно строго определенному кругу людей. Иначе говоря, те све­дения, которые не подлежат разглашению и составляют тайну. Здесь тайна - **субъективная категория** — это сведения, которые какой-то субъект (в его широком понимании) считает необходимым скрыть от других. Если субъект — физическое лицо устанавливает для себя, что об этом факте, например, его каком-то поступке никому рассказывать не будет, то он засекретил для себя эту информа­цию. Или группа заговорщиков замышляет совершить какие-то действия, которые могут быть успешными только в том случае, если об этом их заговоре (например, совершить государственный переворот) никто не будет знать до момента его осуществления.

Деление тайны на субъективную и объективную в некоторой степени условно. Основной критерий такого деления – это кто ус­танавливает, что является тайной. Субъект, установивший, что данная информация является, например, государственной тай­ной, в любой момент может ее рассекретить. Тайна как объектив­ная категория в какой-то мере также является субъективной, так как не познана человечеством как субъектом познания. Но «рас­секретить» эту тайну человечество может только тогда, когда дан­ные явления, законы природы будут познаны и открыты.

Таким образом**, тайна (в области защиты информа­ции) — это субъективная категория, когда сведения о каких-то событиях, явлениях, предметах скрываются по тем или иным со­ображениям собственником (владельцем) информации от посто­ронних лиц.**

Сохранение сведений в тайне, владение секретами дает опре­деленные преимущества той стороне, которая ими владеет.

В законодательстве РФ встречается упоминание более чем о 30 видах различных тайн (государственная, служебная, коммерческая, банковская, личная, семейная тайна, тайна следствия, связи, почтовых отправлений и другие). Общего определения тайны в законодательстве РФ не дано. В Гражданском кодексе РФ существует только определение служебной и коммерческой тайны (статья 139), которое полезно рассмотреть для понимания соотношения различных видов тайн.

Согласно этому определению «информация составляет служебную или коммерческую тайну в случае,

* когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам,
* к ней нет свободного доступа на законном основании и
* обладатель информации принимает меры к охране ее конфиденциальности.

Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

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

С использованием этого определения можно сформулировать **общие признаки тайны**:

1. Информация имеет действительную или потенциальную ценность для обладателя в силу неизвестностиее третьим лицам. Такими лицами могут быть государства, юридические или физические лица.
2. К информации нет свободного доступа на законном основании. Возможность сохранения ее неизвестной для третьих лиц установлена законом.
3. Обладатель информации принимает меры к охране ее конфиденциальности (секретности).

В соответствии с общими признаками ***государственная тайна*** определяется следующими уточняющими признаками:

1. *Кто является владельцем информации?* – Государство.
2. *Насколько велика ценность информации для государства?* – Информация, составляющая государственную тайну, имеет действительную или потенциальную ценность для ее собственника - государства в силу ее неизвестности для третьих государств, юридических и физических лиц. Информация очень ценна. Распространение этой информации может нанести ущерб безопасности государства.
3. *Можно ли ограничить доступ к информации на законном основании?* – Да. К этой информации нет свободного доступа в соответствии с Законом «О государственной тайне», в котором указан перечень сведений, составляющих государственную тайну.
4. *Принимаются ли меры к охране секретности информации?* - Да. Существует реальная система защиты государственной тайны.

Аналогично может быть дано определение и других видов тайн. Например,***для служебной тайны ее признаками являются:***

1. Владельцем информации является также государство.
2. Информация представляет ценность в силу ее неизвестности. Однако размер ущерба от ее открытого распространения не выходит на уровень ущерба безопасности государства. Распространение такой информации может нанести ущерб деятельности отдельных органов государственной власти, местного самоуправления, предприятий и организаций, выполняющих работы по заказу этих органов.
3. Доступ к информации ограничен на законном основании решением органов государственной власти и местного самоуправления.
4. Органы государственной власти, местного самоуправления, предприятия и организации принимают меры по защите информации отнесенной к служебной тайне.

В Федеральном законе « Об информации, информационных технологиях и о защите информации» фактически в качестве синонима понятия тайна применяется понятие ***«информация ограниченного доступа».*** Информация с ограниченным доступом по условиям ее правового режима в Законе подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

***Конфиденциальная информация*** - это не составляющая государственную тайну документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ. Перечень сведений конфиденциального характера, содержащийся в такой информации, определен в Указе Президента РФ от 06. 03 97 г. № 188. К ним относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность *(персональные данные)*, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
2. Сведения, составляющие *тайну следствия и судопроизводства.*
3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами *(служебная тайна).*
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее). Такие сведения именуются также как *профессиональная тайна.*
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами *(коммерческая тайна).*
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Необходимо отметить, что в ряде случаев нет четкой границы между различными видами информации ограниченного доступа. Так, например, сведения, составляющие коммерческую тайну фирмы, при передаче их в органы государственной власти становятся в тоже время служебной тайной этих органов.

**2. Понятие «защищаемая информация» и его соотношение с понятием тайны.**

К защищаемой информации относится:

1. Часть **открытой информации**, определяемая собственником (владельцем). Защита открытой информации направлена не на ограничение доступа к информации, а **на сохранность информации** в рамках установленных правил ее обработки и использования. **Она** **защищается от утраты**.

Защита открытой информации существовала всегда и производилась путем:

* Регистрации ее носителей;
* Учета их движения и местонахождения;
* Создания безопасных условий хранения.
1. **Информация ограниченного доступа** - конфиденциальная информация, в том числе составляющая государственную тайну (**защищается от утечки и утраты).**

**Особенности защищаемой информации ограниченного доступа:**

Информационным процессам присущи определенные законо­мерности. Наиболее общими являются:

* постоянный рост количе­ства информации,
* ее кругооборот,
* рассеяние,
* старение инфор­мации.

**Постоянный рост количе­ства защищаемой информации.** Если информация ограниченного доступа является основанием для созда­ния новой информации (документов, изделий и т.п.), то созданная на этой основе информация является, как правило, также ограниченного доступа, а значит - защищаемой . В отношении конфиденциальной информации, содержащей, в част­ности, коммерческую тайну, этого однозначно сказать нельзя.

**Кругооборот** **защищаемой ин­формации** происходит в определенной, ограниченной режимны­ми мерами сфере — научно-производственной, управленческой, коммерческой и др. Защищаемая информация диктует всем, кто с нею сталкивается, правила обраще­ния с нею, уровень защитных мер к себе и т.д. Уровень защиты информации определяется грифом секретности или конфиденци­альности.

**Старение защищаемой информации** имеет особенности.

Созданная один раз защищаемая информация (как и несекрет­ная) может быть использована многократно в течение неограни­ченного времени сколь угодно большим количеством потребите­лей. Она обладает способностью не уничтожаться, не убывать со временем и по мере использования, а даже возрастать, то есть порождать новую информацию. Следует отметить, что эта зако­номерность, присущая всей информации, создает объективные предпосылки определенной уязвимости защищаемой информа­ции: если кто-то позаимствовал секретные сведения без наруше­ния физической целостности носителя (произошла, как говорят, утечка секретной информации), то собственник этой информа­ции может об этом не узнать вообще или узнать из других источ­ников информации.

**Рассеяние информации**. Рассеяние открытой информации носит, как известно, случайный характер. Рассеяние защищаемой информации производится только детерминированно: заранее определяется возможное количество потребителей для засекреченной информации, в соответствии с которым размножается определенное количество экземпляров со­ответствующего документа, которые и рассылаются заранее опре­деленным адресатам.

 Таким образом, понятие защищаемой информации – более широкое, чем понятие информации ограниченного доступа и понятия тайны. В него, кроме названных категорий информации, защищаемых от утечки и утраты, включается открытая информация, защищаемая от утраты.

**3. Критерии отнесения открытой информации к защищаемой.**

При решении вопроса об отнесении конкретной информации к защищаемой нужно руководствоваться определенными критериями, т.е. признаками, при наличии которых информация может быть отнесена к защищаемой.

 Общей основой для отнесения информации к защищаемой является **ценность информации**, поскольку именно ценность информации диктует необходимость ее защиты. Поэтому критерии отнесения информации к защищаемой являются по существу критериями определения ее ценности.

Критерии отнесения открытой информации к защищаемой:

* Необходимость информации для правового обеспечения деятельности предприятия (документированная информация, регламентирующая статус предприятия, права, обязанности и ответственность его работников);
* Необходимость информации для производственной деятельности (информация, относящаяся к научно-исследовательской, проектной, конструкторской, технологической, торговой и другим сферам производственной деятельности);
* Необходимость информации для управленческой деятельности (информация, требующаяся для принятия управленческих решений, для организации производственной деятельности и обеспечения ее функционирования);
* Необходимость информации для финансовой деятельности;
* Необходимость информации для обеспечения функционирования социальной сферы;
* Необходимость информации как доказательного источника на случаи возникновения конфликтных ситуаций;
* Важность информации как исторического источника, раскрывающего направления и особенности деятельности предприятия.

Эти критерии обусловливают необходимость защиты открытой информации от утраты.

**4. Критерии отнесения конфиденциальной информации к защищаемой.**

Названные выше критерии отнесения открытой информации к защищаемой вызывают потребность в защите **от утраты** и конфиденциальной информации.

 Однако основной, определяющий критерий отнесения информации к конфиденциальной и защиты ее от утечки – **возможность получения** **преимуществ от использования информации за счет неизвестности ее третьим лицам**.

 Этот критерий имеет две составляющие:

1. **Неизвестность информации третьим лицам.**
2. **Получение** **преимуществ от использования информации** (получение выгоды, предотвращение политического, экономического или морального ущерба).

Эти две составляющие взаимосвязаны и взаимообусловлены:

 С одной стороны, неизвестность информации третьим лицам сама по себе ничего не значит, если не обеспечивает преимуществ тому, кто ее защищает.

 С другой стороны, преимущества можно получить только за счет такой неизвестности.

**5. Условия отнесения информации к защищаемой.**

При отсутствии названных выше критериев нет оснований для перевода информации в категорию защищаемой. **Но наличие этих критериев не означает, что информация во всех случаях без исключения должна быть отнесена к защищаемой.** Критерии – лишь объективные **показатели возможности** отнесения информации к защищаемой. Для реализации этой возможности в действительности необходимы следующие **условия**:

1. **Если** информация не является общедоступной на законном основании, т.е. не содержит сведений, которые **запрещено** относить к конфиденциальным. Перечни таких сведений содержатся в нескольких нормативных актах: законах «О государственной тайне», «О коммерческой тайне», «Об информации, информатизации и защите информации», «О благотворительной деятельности и благотворительных организациях», Постановлении Правительства от 5 декабря 1991 года №35 «О перечне сведений, которые не могут составлять коммерческую тайну», «Положении о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

2. **Если** имеются технические возможности для защиты носителей информации. Речь идет об объектах, которые практически невозможно скрыть от технических средств обнаружения и фиксации, особенно спутниковых.

3. **Если** затраты на защиту информации не превысят количественных и качественных показателей преимуществ, получаемых при ее защите.

 Таким образом, правовой и методологической основой для разработки перечней сведений, составляющей различные виды тайн, являются:

* критерии отнесения информации к защищаемой;
* условия отнесения информации к защищаемой;
* понятие соответствующего вида тайны (их характеристики и показатели)

Специфика предприятия (для коммерческой тайны): то, что для одних является коммерческой тайной, для других – рекламной информацией.

**Литература**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. Анин Б.Ю. Защита компьютерной информации. Петербург, 2010. - 384с.
4. Галатенко В.А. Барсуков В.С., Водолазний В.В. Современные технологии безопасности. - М.: «Нолидж», 2009. - 496 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
7. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция № 8**

**ГОСУДАРСТВЕННАЯ ТАЙНА**

1 Понятие государственной тайны.

2. Правовые основы государственной тайны в РФ.

3. Цели защиты государственной тайны.

4. Объекты защиты.

Сведения, которые не могут составлять государственную тайну.

5. Угрозы информации, составляющей государственную тайну, и их источники.

6. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений. Степени секретности сведений, составляющих государственную тайну.

**1. Становление и понятие государственной тайны.**

 Определение сформулировано в Законе «О государственной тайне»: «**Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации».**

 Очевидно, что в этом определении закреплены главные признаки государственной тайны:

1. Ее собственником является государство (содержится в названии тайны).
2. Области деятельности, в которых может быть информация, составляющая государственную тайну, - военная, внешнеполитическая, экономическая, разведывательная, контрразведывательная и оперативно-розыскная деятельность.
3. Охрана государственной тайны возложена на государство.
4. Критерий отнесения информации к гостайне – распространение этих сведений может нанести ущерб безопасности РФ.

**2. Правовые основы государственной тайны.**

***Основные направления государственной политики в области защиты государственной тайны.*** *Государственная политика в области защиты государственной тайны определяется законами общего характера* (Конституцией Российской Федерации, Законом “О безопасности”, кодексами), *специальными (базовыми) законами в области защиты государственной тайны* (“О государственной тайне”) и другими нормативными правовыми актами Российской Федерации.

 *Основными направлениями проведения государственной политики в области защиты государственной тайны являются:*

* создание в органах государственной власти и местного самоуправления, на предприятиях, их объединениях, в учреждениях и организациях, использующих информацию, составляющую государственную тайну, специальных подразделений по защите государственной тайны и систем защиты информации;
* осуществление государственного заказа на проведение работ в области защиты государственной тайны;
* лицензирование деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны;
* сертификация средств защиты информации, составляющей государственную тайну, а также систем и средств информатизации и связи, обрабатывающих секретную информацию, по требованиям безопасности информации;
* создание единой системы законодательных, организационно-распорядительных, нормативных, планирующих и информационных документов, регламентирующих и обеспечивающих деятельность в области защиты государственной тайны;
* контроль за выполнением установленных требований по защите государственной тайны и надзор за соблюдением законности в области защиты государственной тайны.

Законодательно закреплено, что деятельность предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, является важнейшим видом основной деятельности.

Рассмотрим понятия, которые важны для понимания концепции защиты государственной тайны.

***Безопасность*** - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Более «техническим» определением этого термина, которое позволяет перейти к количественной оценке уровня безопасности, может быть следующее.

Безопасность - это состояние, при котором отсутствует недопустимый риск нанесения неприемлемого ущерба кому-либо. В таком определении учтены два фактора, определяющие безопасность. Во-первых, безопасность не может быть абсолютной. Всегда существует определенный риск (вероятность) возникновения угроз и нанесения некоторого ущерба. Во-вторых, уровень безопасности зависит от величины возможного ущерба. Таким образом, состояние безопасности определяется двумя показателями: риском (вероятностью) возникновения ущерба и величиной этого ущерба в том или ином измерении.

***Под безопасностью государства*** следует понимать состояние защищенности его политических, экономических, военных, научно-технических и других интересов от внутренних и внешних угроз.

***Жизненно важные интересы*** - совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

***К основным объектам безопасности относятся***: личность - ее права и свободы; общество - его материальные и духовные ценности; государство - его конституционный строй, суверенитет и территориальная целостность

***Основным субъектом обеспечения безопасности является государство***, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей.

***Полномочия субъектов обеспечения защиты государственной тайны.*** Государство не берет на себя всей полноты ответственности по защите государственной тайны, оно лишь обеспечивает создание необходимых и достаточных условий эффективной защиты государственной тайны. Предприятия, учреждения, организации, граждане непосредственно обеспечивают ее защиту в соответствии с действующими законами и утвержденными полномочными органами требованиями.

***Угроза безопасности*** - совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, определяет содержание деятельности по обеспечению внутренней и внешней безопасности.

***Угрозы безопасности государства*** могут существовать в различных сферах его жизнедеятельности.

1. Угрозы, влияющие на политический потенциал государства.
2. Угрозы, влияющие на экономический потенциал государства.
3. Угрозы, влияющие на научно-технический потенциал государства.
4. Угрозы, влияющие на оборонный потенциал государства.
5. Угрозы, влияющие на военный потенциал государства.

Закон «О безопасности» определяет состав сил обеспечения безопасности, которые, в частности, включают в себя ***службы обеспечения безопасности*** средств связи и информации, таможни природоохранительные органы, органы охраны здоровья населения и другие государственные органы обеспечения безопасности, действующие на основании законодательства. Это положение Закона определяет ***правовую базу создания подразделений защиты государственной тайны*** в органах государственной власти, местного самоуправления, на предприятиях и организациях.

**«Концепция защиты государственной тайны в Российской Федерации»** представляет собой систему взглядов на проблему защиты государственной тайны, определяет основную идею и пути ее решения в различных сферах деятельности государства.

Положения Концепции используются при определении политики государства в рассматриваемой области защиты информации, при планировании и выполнении конкретных мероприятий по защите государственной тайны.

В Концепции излагаются существующие проблемы в области защиты государственной тайны, цели и задачи защиты, основные принципы организации и осуществления защиты государственной тайны, а также направления совершенствования системы защиты государственной тайны.

Полное содержание Концепции, как правило, не может быть изложено в одном официальном документе, а представлено в нескольких взаимосвязанных документах. Применительно к вопросу защиты государственной тайны такими документами являются Конституция РФ, Закон РФ, «О безопасности», Концепция национальной безопасности, Закон «О государственной тайне».

**3. Цели защиты государственной тайны**

Общей целью защиты государственной тайны является ***предотвращение или снижение величины ущерба безопасности государства***путем исключения (существенного затруднения) утечки информации по всем возможным каналам: в результате ведения агентурной и технической разведки, в результате различного рода публикаций, общения людей, обмена информацией в открытых телекоммуникационных системах, несанкционированного доступа к информации и т. д.

Деятельность по защите государственной тайны может быть направлена на предотвращение и локализацию реального ущерба от существующих угроз безопасности информации для конкретных объектов, а также на создание условий для предотвращения потенциального ущерба безопасности государства, который может проявиться в будущем.

Основными целями защиты государственной тайны в различных сферах деятельности государства являются:

***в военной области***

предотвращение снижения эффективности группировок войск (сил), образцов вооружения и военной техники, систем управления войсками (силами) и оружием; путем исключения (существенного затруднения) утечки сведений, составляющих государственную тайну, знание которых позволяет реализовать потенциальному противнику военно-технические контрмеры;

обеспечение выгодных с позиции защиты государственной и тайны условий подготовки и реализации международных договоров по сокращению вооружений и вооруженных сил, контроля их выполнения;

обеспечение скрытности важнейших мероприятий по переводу страны с мирного на военное положение в особый период;

***во внешнеполитической области***

предотвращение ущерба от утечки информации о возможных направлениях, стратегии и тактике внешнеполитической деятельности России;

обеспечение паритета в области информированности сторон на международных переговорах;

***в экономической области***

предотвращение экономического ущерба государству путем исключения существенного затруднения) утечки сведений о закупках товаров в государственный резерв и их выделении из этого резерва для продажи, объемах закупок товаров для государственных нужд, состоянии расчетов с иностранными государствами, перспективах валютных поступлений;

обеспечение выгодных (с позиции защиты государственной тайны) условий заключения экономических договоров, размещения совместных предприятий;

предотвращение снижения эффективности экономической деятельности важнейших для экономики страны предприятий путем исключения (существенного затруднения) утечки защищаемой информации;

сохранение в тайне от иностранных государств мобилизационных возможностей отраслей хозяйства;

предотвращение несанкционированного доступа к информации о состоянии и перспективах использования сырьевых и материально-технических ресурсов государства.

предотвращение несанкционированного доступа к информации о научно-технических достижениях, определяющих военную и технологическую безопасность государства;

предотвращение ущерба от утечки информации о результатах фундаментальных и поисковых исследований, передовых технологиях и перспективных материалах, имеющих оборонное и двойное применение;

***в области разведывательной, контрразведывательной и оперативно-розыскной деятельности***

предотвращение ущерба от утечки информации о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности;

предотвращение ущерба от утечки информации о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

предотвращение ущерба от утечки информации о методах и средствах защиты секретной информации, об организации и о фактическом состоянии защиты государственной тайны.

**4. Объекты защиты**

При защите государственной тайны объектами защиты являются носители сведений, составляющих государственную тайну, независимо от физической природы носителя. Существуют три класса таких носителей:

1. Носители, хранящие записи «готовой информации», то есть информации, непосредственно раскрывающей сведения, составляющие государственную тайну. К ним относятся бумажные носители, магнитные носители, оптические носители и т.д.
2. Носители «готовой информации» информации в процессе ее передачи. К ним можно отнести всевозможные системы связи.
3. Носители признаков проявления сведений, составляющих государственную тайну, или так называемых демаскирующих признаков объектов защиты. Демаскирующие признаки могут быть непосредственно присущи объекту или проявляться в виде следов деятельности объектов. Носителями демаскирующих признаков могут быть образцы вооружения, технологические процессы, защищаемые природные ресурсы и другие носители.

**5. Угрозы информации, составляющей государственную тайну, и их источники.**

К основным угрозам относятся:

1. ***Разглашение информации***, то есть несанкционированное доведение защищаемой информации до субъектов, не имеющих право доступа к этой информации.
2. ***Ведение разведки*** относительно сведений, составляющих государственную тайну. Такая разведка может быть агентурной или технической. *Агентурная разведка* - вид разведывательной деятельности, осуществляемой с помощью агентов. Под агентом понимается сотрудник разведки или организации, внедренный на объект защиты и занимающейся деятельностью, направленной на добывание защищаемой информации. *Техническая разведка* - деятельность, направленная на добывание защищаемой информации с помощью технических средств. Техническая разведка по местонахождению носителей разведывательной аппаратуры подразделяется на виды: воздушная разведка; космическая разведка; морская разведка; наземная разведка.
3. ***Несанкционированный доступ*** к информации - доступ к защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. При этом под доступом понимается получение субъектом возможности ознакомления с информацией и/или воздействия на нее, в том числе при помощи технических средств. Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать: государство, юридическое лицо; группа физических лиц, в том числе общественная организация; отдельное физическое лицо.
4. ***Несанкционированные и*** ***непреднамеренные воздействия*** на информацию, приводящие к искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. Особая опасность этих угроз состоит в том, что их реализация может создавать условия для несанкционированного доступа к информации.

***Источники угроз для информации, составляющей государственную тайну.***

*Внешние:*

деятельность иностранных разведывательных служб (органов);

деятельность иностранных экономических структур;

деятельность иностранных преступных групп и отдельных лиц;

*Внутренние:*

противоправная деятельность общественных, экономических и других структур;

деятельность преступных групп и отдельных лиц;

природные явления;

сбои и отказы техники;

ошибки персонала.

**6. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений.**

*Отнесение сведений к государственной тайне и их засекречивание – это введение в предусмотренном Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.* В этом определении учитываются два принципиальных этапа защиты государственной тайны.

*На первом этапе* принимается решение об отнесении сведений к государственной тайне, которое является основанием для введения ограничений на их распространение.

*На втором этапе* принимаются всесторонние меры по защите государственной тайны, направленные на ограничение доступа к носителям сведений, составляющих государственную тайну.

Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами *законности, обоснованности и своевременности.*

***Законность*** отнесения сведений к государственной тайне и их засекречивания заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 Закона «О государственной тайне» и законодательству Российской Федерации о государственной тайне. Законодательство устанавливает два вида норм, регламентирующих процедуру отнесения сведений к государственной тайне и их засекречивания.

Нормы первого вида устанавливают *Перечень сведений, составляющих государственную тайну.*

Нормы второго вида определяют *Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.* Деятельность по защите государственной тайны может осуществляться только в пределах этих установленных законодательством рамок.

***Обоснованность*** отнесения сведений к государственной тайне и их засекречивания заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан. При принятии решения об отнесении сведений к государственной тайне и их засекречивании должны всесторонне взвешиваться положительные и отрицательные последствия этого шага для интересов государства, общества и граждан.

***Своевременность***отнесения сведений к государственной тайне и их засекречивания заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно. *Принцип своевременности* также означает необходимость заблаговременной разработки мер защиты государственной тайны, а также возможности их оперативной корректировки при изменении угроз, условий защиты и важности защищаемой информации. Реализация этого принципа требует создания гибко управляемой системы защиты государственной тайны, обеспечивающей прогнозирования и выявление угроз, их упреждающую нейтрализацию, быструю ликвидацию последствий угроз. Решению этих задач способствует должная степень автоматизации средств и систем защиты информации наличие оперативной системы контроля состояния защиты государственной тайны.

**Литература**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
4. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
5. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция №9**

**Коммерческая тайна**

1. Понятие коммерческой тайны.

2. Сведения, которые не могут составлять коммерческую тайну.

3. Примерный перечень сведений, составляющих коммерческую тайну организации.

4. Степени конфиденциальности сведений, составляющих коммерческую тайну.

5. Понятие режима коммерческой тайны.

6. Права обладателя информации, составляющей коммерческую тайну.

**1. Становление и понятие коммерческой тайны**

**В Гражданском кодексе РФ** изложены основания отнесения информации к коммерческой тайне: Информация составляет коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

**В** **Перечне сведений конфиденциального характера, утвержденном Указом Президента РФ от 6.03.97г. № 188**, к коммерческой тайне отнесены «сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами».

Последнее определение коммерческой тайны дано **в Федеральном законе «О коммерческой тайне» от 29 июля 2004 года**: «**Коммерческая тайна** - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду».

В законе дается также определение информации, составляющей коммерческую тайну. **Информация, составляющая коммерческую тайну -** «научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны».

**2. Сведения, которые не могут составлять коммерческую тайну.**

В Федеральном законе «О коммерческой тайне» от 29 июля 2004 года в статье 5 перечислены с**ведения, которые не могут составлять коммерческую тайну.** К ним относятся:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

**3. Примерный перечень сведений, составляющих коммерческую тайну организации.**

1. ПРОИЗВОДСТВО.

Сведения о структуре и масштабах производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов, комплектующих и готовой продукции.

1. УПРАВЛЕНИЕ.

Сведения о применяемых оригинальных методах управления организацией (фирмой). Сведения о подготовке. Принятии и исполнении отдельных решений руководства фирмы по коммерческим, организационным и др. вопросам.

1. ПЛАНЫ.

Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях, сведения о планах инвестиций, закупок и продаж.

1. СОВЕЩАНИЯ.

Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления организации.

1. ФИНАНСЫ.

Сведения о кругообороте средств организации, финансовых операциях, состоянии банковских счетов организации и проводимых операциях, об уровне доходов организации, о состоянии кредитов организации (пассивы и активы). Главная книга организации.

1. РЫНОК.

Сведения о применяемых фирмой оригинальных методах изучения рынка (маркетинга). Сведения о результатах сегментации рынка, содержащие оценки состояния и перспектив развития рыночной конъюнктуры. Сведения о рыночной стратегии фирмы, о применяемых ею оригинальных методах осуществления продаж, об эффективности служебной или коммерческой деятельности фирмы.

1. ПАРТНЕРЫ.

Обобщенные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах, состоящих в деловых отношениях с организацией.

1. КОНКУРЕНТЫ.

Обобщенные сведения о внутренних и зарубежных предприятиях как потенциальных конкурентах, оценка качества деловых отношений с конкурирующими предприятиями.

1. ПЕРЕГОВОРЫ.

Сведения о подготовке, проведении и результатах переговоров с деловыми партнерами.

1. КОНТРАКТЫ.

Сведения об условиях конфиденциальности, из которых можно установить порядок соглашения и другие обязательства организации с партнерами, клиентами.

1. ЦЕНЫ.

Сведения о методах расчета, структуре, уровне реальных цен на продукцию и размеры скидок.

1. ТОРГИ, АУКЦИОНЫ.

Сведения о подготовке к участию в торгах и аукционах, результатах приобретения или продажи на них товаров.

1. НАУКА И ТЕХНИКА.

Сведения о целях, задачах, программах перспективных научных исследований. Ключевые идеи научных разработок, параметры разрабатываемых технологических процессов (размеры, объемы, конфигурации и др.). Данные об условиях экспериментов и оборудовании, на котором они проводились. Сведения о материалах, из которых изготовлены отдельные детали, об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный эффект. Сведения о методах защиты от подделки товарных и фирменных знаков, о состоянии парка ПЭВМ и программного обеспечения.

1. ТЕХНОЛОГИЯ.

Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения, об условиях их производства и транспортировке продукции.

1. БЕЗОПАСНОСТЬ.

Сведения о порядке и состоянии организации защиты служебной или коммерческойй тайны, о порядке и состоянии организации охраны, системы сигнализации, пропускном режиме. Сведения, составляющие служебную или коммерческую тайну организаций, предприятий-партнеров и передаваемые ими в пользование на доверительной основе.

**4. Степени конфиденциальности сведений, составляющих коммерческую тайну.**

Если в отношении государственной тайны законом «О государственной тайне» установлено три степени секретности (Особой важности, совершенно секретно и секретно), то закон о «О коммерческой тайне» гласит, что на документах, **предоставляемых органам государственной власти, иным государственным органам, органам местного самоуправления** и содержащих информацию, составляющую коммерческую тайну, «должен быть нанесен **гриф "Коммерческая тайна"** с указанием ее обладателя (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства)».

**В процессе функционирования на предприятии** коммерческая информация может быть ранжирована по сте­пени ее важности для предприятия с тем, чтобы регулировать ее распространение среди работающих на предприятии, указывать пользователей этой информации, уровень ее защиты и т.д. Для обозначения степени важности коммерческой информации для предприятия предлагаются разные системы обозначения степени ее конфиденциальности (грифы конфиденциальности):

Например:

коммерческая тайна — строго конфиденциально (КТ — СК);

коммерческая тайна — конфиденциально (КТ — К);

коммерческая тайна (КТ).

Предлагаются также двухуровневые системы ранжирования коммерческой информации по степени важности: «Коммерческая тайна» и «Для служебного пользования» («ДСП»).

**5. Понятие режима коммерческой тайны**

**Режим коммерческой тайны** - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности (ст.3 ФЗ «О коммерческой тайне»)

**Меры по охране конфиденциальности информации**, принимаемые ее обладателем, в соответствии со ст.10 закона 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 только после принятия обладателем информации, составляющей коммерческую тайну, названных мер.

**6. Права обладателя информации, составляющей коммерческую тайну**

 Права обладателя информации, составляющей коммерческую тайну закреплены ст.7 ФЗ «О коммерческой тайне»:

1. Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны.

2. Обладатель информации, составляющей коммерческую тайну, имеет право:

1) устанавливать, изменять и отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

4) вводить в гражданский оборот информацию, составляющую коммерческую тайну, на основании договоров, предусматривающих включение в них условий об охране конфиденциальности этой информации;

5) требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

6) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;

7) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

**Рекомендуемая литература**

Основные источники:

**Литература**

1. О коммерческой тайне: Федеральный закон №86-ФЗ от 29 июля 2004 года
2. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
3. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
4. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
5. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
6. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция №10**

**Персональные данные**

1. Понятие персональных данных.

2. Субъекты правоотношений в области персональных данных.

3. Требования к защите персональных данных.

**1. Понятие персональных данных**

 **Персональные данные** – это особый институт охраны права на неприкосновенность частной жизни. Неприкосновенность частной жизни гражданина и уважение к ней – это составная часть реализации его личной свободы, которая включает:

* Право на свободу располагать собой;
* Право на тайну частной жизни;
* Право на тайну корреспонденции;
* Право на свободу мысли, совести и вероисповедания;
* Право на свободное выражение своего мнения;
* Право на защиту личности (своего имени, чести, достоинства и деловой репутации, своей национальной принадлежности);
* Право на защиту жилища, право на тайну голосования.

Всеобщая декларация прав человека (ст.1) начинается словами: Все люди рождаются свободными и равными в своем достоинстве и правах». Право на неприкосновенность частной жизни является одним из конституционных прав человека. Конституционными гарантиями являются**:**

* Конституционный запрет осуществлять сбор, хранение, использование и распространение информации о частной жизни лица без его согласия (ст.24);
* Конституционная обязанность органов государственной власти и органов местного самоуправления обеспечить каждому возможность ознакомления с документами и материалами, затрагивающими его права и свободы (ст.24) и др.

Информация, затрагивающая неприкосновенность частной жизни, лица и ставшая известной на законных основаниях другим лицам, должна охраняться:

* В режиме профессиональной тайны – если она получена ими исключительно в силу исполнения своих профессиональных обязанностей, не связанных с государственной или муниципальной службой;
* В режиме служебной тайны – если она получена представителями государственных органов или органов местного самоуправления в силу исполнения своих служебных обязанностей.

Как следует из Доктрины информационной безопасности РФ, права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, закрепленные в Конституции РФ, практически не имеют достаточного правового, организационного и технического обеспечения. Это проявляется, в частности, в том, что неудовлетворительно организована защита данных о физических лицах **(персональных данных),** собираемых федеральными органами власти, органами власти субъектов федерации, органами местного самоуправления.

Проблема персональных данных стала особенно актуальной в связи с созданием и использованием баз данных о гражданах в компьютерных сетях государственных и негосударственных структур. Естественным образом встала задача обеспечения неприкосновенности частной

В Европе для охраны и защиты права на неприкосновенность частной жизни в условиях автоматизированной обработки личных данных о гражданах более 30 лет назад был введен особый институт правовой охраны личности – институт защиты персональных данных. Более чем в 20 европейских государствах приняты национальные законы о персональных данных, в ряде стран введены уполномоченные по защите персональных данных, во всех странах Европейского Союза с 1998 г. создана единая унифицированная система защиты персональных данных, в том числе в секторе телекоммуникаций.

Федеральный закон «Об информации, информатизации и защите информации» вводит и определяет понятие персональных данных (ст.2): **Информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.**

**Трудовой кодекс РФ** определяет **персональные данные работника как информацию, необходимую работодателю в связи с трудовыми отношениями и касающуюся конкретного работника.**

**Проект закона «О персональных данных**» дает следующее определение персональных данных: **Персональные данные – любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу.**

При этом ни один закон не определяет состава персональных данных. Федеральный закон «Об информации, информатизации и защите информации» относит персональные данные к конфиденциальной информации и устанавливает, что перечни персональных данных должны быть закреплены федеральным законом (Ст.11). Однако такой закон до сих пор не принят.

Ученые же считают, что к персональным данным могут быть отнесены сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам:

* Биографические и опознавательные данные (в том числе об обстоятельствах рождения, усыновления, развода);
* Личные характеристики (в том числе о личных привычках и наклонностях);
* Сведения о семейном положении (в том числе о семейных отношениях);
* Сведения об имущественном, финансовом положении (кроме случаев, прямо установленных в законе);
* Сведения о состоянии здоровья

Следует отметить, **что такие сведения становятся персональными данными, когда они находятся не у лица, к которому относятся, а у уполномоченных на то юридических и физических лиц.** Сведения, относящиеся к персональным данным, могут и не являться личной тайной субъекта, однако при этом будут охраняться уполномоченными на то лицами.

**2. Субъекты правоотношений в области персональных данных.**

Субъектами права в области персональных данных выступают:

* **субъекты персональных данных** – лица, к которым относятся соответствующие данные, и их наследники;
* **держатели персональных данных** – органы государственной власти и органы местного самоуправления, юридические и физические лица, осуществляющие на законных основаниях сбор, хранение, передачу, уточнение, блокирование, обезличивание, уничтожение персональных данных.

Субъект персональных данных в соответствии с Трудовым кодексом РФ в отношении своих данных имеет право:

* на полную информацию об их персональных данных и обработке этих данных;
* на свободный доступ к своим персональным данным;
* уточнять свои персональные данные;
* требовать об исключении своих персональных данных;
* обжаловать неправомерные действия или бездействия в отношении персональных данных.

Ограничение права на свои персональные данные возможно в случаях:

* если субъект персональных данных допущен к сведениям, составляющим гостайну;
* если персональные данные получены в результате оперативно-розыскной деятельности; если субъект задержан по подозрению в совершении преступления либо ему предъявлено обвинение по уголовному делу.

Государство может регулировать действия держателей персональных данных в формах:

* лицензирования действий с персональными данными;
* регистрации баз персональных данных;
* регистрации держателей персональных данных;
* сертификации информационных систем, предназначенных для обработки персональных данных.
1. **3. Требования к защите персональных данных**

Закон «Об информации, информатизации и защите информации» требует, чтобы деятельность негосударственных организаций и частных лиц по обработке и предоставлению персональных данных, равно как и по проектированию, производству средств защиты информации и обработки персональных данных обязательно лицензировались в порядке, установленном Правительством РФ; а также декларирует, что персональные данные должны защищаться, а режим защиты в отношении персональных данных устанавливается Федеральным законом.

В Трудовом кодексе РФ защите персональных данных посвящена Глава 14. Требования к работе с персональными данными, закрепленные в ТК РФ, записаны и в законопроекте «О персональных данных», принятом в первом чтении:

1. Персональные данные должны быть получены и обработаны законным способом.
2. Персональные данные включаются в базы персональных данных на основании свободного согласия субъекта, выраженного в письменной форме, за исключением случаев, прямо установленных в законе.
3. Персональные данные должны накапливаться для точно определенных и законных целей, не использоваться в противоречие с этими целями и не быть избыточными по отношению к ним. Не допускается объединение баз персональных данных, собранных держателями в разных целях, для автоматизированной обработки информации.
4. Персональные данные, предоставляемые держателем, должны быть точными и в случае необходимости обновляться.
5. Персональные данные должны храниться не дольше, чем этого требует цель, для которой они накапливаются, и подлежать уничтожению, когда эта цель достигнута или в ней миновала надобность.
6. Персональные данные охраняются в режиме конфиденциальной информации, исключающем их случайное или несанкционированное разрушение или случайную их утрату, а также несанкционированный доступ к данным, их изменение, блокирование или передачу.
7. Для лиц, занимающих высшие государственные должности, и кандидатов на эти должности, может быть установлен специальный правовой режим для их персональных данных, обеспечивающий открытость только общественно значимых данных.
8. Режим конфиденциальности персональных данных снимается: в случаях обезличивания персональных данных; и по желанию субъекта.
9. Запрещаются любые действия с персональными данными, раскрывающими расовое или этническое происхождение, национальную, языковую, партийную, религиозную принадлежность.
10. При получении персональных данных в государственных органах и органах местного самоуправления их охрана обеспечивается в режиме служебной тайны.

**Литература**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
4. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
5. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция 11**

**Состав и классификация носителей защищаемой информации**

1. Понятие носителей защищаемой информации и их классификация.

2. Документ как носитель защищаемой информации.

3. Изделия (предметы) как носители защищаемой информации.

4. Вещества и материалы как носители защищаемой информации.

5. Электромагнитные, тепловые, радиационные и другие излучения как носители защищаемой информации.

**1. Понятие носителей защищаемой информации и их классификация**

Материальные объекты, в том числе физические поля, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, создавая тем самым возможность для ее накопления, хранения, передачи и использования, называются **носителями информации.**

Для записи как секретной, так и несекретной информации используются одни и те же но­сители .

Как правило, носители секретной и конфиденциальной ин­формации охраняются собственником этой информации. Это вы­звано тем, что если к ним получит несанкционированный доступ соперник или лицо, от которого эта информация охраняется, то носитель может стать источником информации, из которого это

лицо может незаконно добыть интересующую его и защищаемую от него информацию.

Носители защищаемой информации можно классифицировать следующим образом:

* документы;
* изделия (предметы);
* вещества и материалы;
* электромагнитные, тепловые, радиационные и другие излучения;
* гидроакустические, сейсмические и другие поля;
* гео­метрические формы строений, их размеры и т.п.

В качестве носителя защищаемой информации выступает также **человек,** мозг которого представляет исключительно слож­ную систему, хранящую и перерабатывающую информацию, по­ступающую из внешнего мира. Свойство мозга отражать и позна­вать внешний мир, накапливать в своей памяти колоссальные объемы информации, в том числе и секретной, естественно, ста­вят человека на первое место как носителя конфиденциальной информации. Человек как хранитель секретной и конфиденци­альной информации обладает возможностью (кроме получения такой информации извне) генерировать новую информацию, в том числе секретную. У него как носителя защищаемой инфор­мации могут быть отмечены как позитивные черты, так и нега­тивные.

Положительно то, что без согласия субъекта — носителя защи­щаемой информации, или, как еще говорят, секретоносителя, из его памяти, как правило, никакая информация не может быть извлечена. Он может давать оценку важности имеющейся у него в памяти информации и в соответствии с этим обращаться с нею. Он может ранжировать и потребителей защищаемой информа­ции, то есть знать, кому и какую информацию он может доверить.

В то же время он может заблуждаться в отношении истинности потребителя защищаемой информации, или встать на путь созна­тельного не сохранения доверенной ему по службе или работе сек­ретной или конфиденциальной информации: совершить государ­ственную измену (шпионаж, выдача государственной или служеб­ной тайны врагу и т.п.) или разболтать секреты своим знакомым и родственникам. В сфере защиты информации человек имеет статус **субъекта информационных отношений.**

**2. Документ как носитель защищаемой информации**

**Документ — зафиксированная на материальном носителе ин­формация с реквизитами, позволяющими ее идентифицировать.** По форме документы как носители информации могут быть са­мыми разнообразными:

* бумага,
* кино- и фотопленка,
* внутренний накопитель на жестком магнитном или магнито - оптическом диске (НЖМД или НМОД - винчестер);
* внешний накопитель на жестком магнитном диске (ЗИП-драйвер);
* внешнее устройство накопления информации (стриммер);
* накопитель на магнитной ленте или специальной металлической нити (в кассетах или бобинах);
* гибкий магнитный диск (ГМД - дискета);
* оптический или магнитооптический диск (лазерный или компакт - диск);
* бумажная (картонная), пластиковая или металлическая карта;
* интегральная микросхема памяти (ИМСП) - микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы памяти ЭВМ и других компьютерных устройств, элементы и связи которого неразрывно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие;
* листинг - распечатка компьютерной информации на твердом физическом носителе (бумаге или пленке) и др.

Информа­ция, записанная на носителе, может быть в виде текста, чертежей, формул, графиков, карт и т.п.

Классификация материальных носителей информации

1. По времени хранения информации:

* *оперативные* - обеспечивающие кратковременное хранение данных и команд, например, оперативное запоминающее устройство (ОЗУ) или электромагнитное поле;
* *постоянные* - время хранения информации ограничивается лишь сроком службы (физическим износом) материала МНИ, например, постоянное запоминающее устройство (ПЗУ) или магнитная лента.

2. По условиям корректировки информации:

* *не перезаписываемые* - МНИ, на которые информация записывается один раз и хранится постоянно до момента физического уничтожения или полного старения (износа) ее носителя - позволяют использовать информацию без корректировки только в режиме "чтение", например, перфокарта, перфолента, карта со штрих-кодом, не перезаписываемый оптический диск (компакт-диск), не перезаписываемая ИМСП;
* *однократно перезаписываемые* - машинные носителя, позволяющие произвести одноразовую корректировку ранее записанной на них информации - информация на них записывается частями (порциями, импульсами) до тех пор, пока объем свободной памяти не будет исчерпан, либо один раз с одновременной перезаписью всех ранее записанных данных, например, интегральная микросхема ПЗУ ЭВМ или иного компьютерного устройства;
* *многократно перезаписываемые* - МНИ, допускающие многократную перезапись и чтение компьютерной информации, например, магнитные диски и ленты, магнитооптические диски, интегральная микросхема ОЗУ, электромагнитное поле.

На документе — носителе защищаемой информации указыва­ется степень закрытости информации (гриф секретности), поэтому потребитель, имея такие данные на руках, может знать кому и как с этой информацией обращаться.

Уровень защиты секретных документов может быть организован с учетом важности содержа­щихся в них охраняемых сведений.

**Слабыми свойствами** документа как носителя защищаемой информации являются следующие. Если к документу получил не­санкционированный доступ недобросовестный потребитель, то он может воспользоваться информацией в своих целях (если она не зашифрована). Документ может быть также утрачен: похищен или уничтожен, испорчен и т.д. За документальной информацией чаще охотятся и иностранные разведки.

**3. Изделия (предметы) как носители защищаемой информации.**

Изделия (предметы) как носители защищаемой информации также довольно распространены. Под ними понимаются:

* засекре­ченные образцы и комплексы вооружения, военной и другой тех­ники;
* оборудование;
* функциональные системы, агрегаты, прибо­ры, входящие в состав комплексов или образцов;
* комплектующие элементы — сборочные единицы и детали, не имеющие самосто­ятельного эксплуатационного назначения и предназначенные для выполнения соответствующих функций в составе оборудования, образцов вооружения, военной и другой техники.

Выполнение ими функций носителей информации осуществляется попутно с выполнением этими изделиями своего основного назначения.

Является ли то или иное изделие секретным, может определить только специалист, особенно, если это касается каких-то ком­плектующих элементов или оборудования.

**4.. Вещества и материалы как носители защищаемой информации.**

Материалы и вещества при определенных условиях также могут выступать в качестве носителей защищаемой информации. В их числе можно назвать:

* конструкционные и эксплуатационные материалы, полуфабрикаты, сырье, топливо и т.д., применяемые при изготовлении и эксплуатации техники и ее элементов. На­пример, термостойкие покрытия космического корабля.
* отходы режимных предприятий (вода, воздух, осадки на земле вокруг объекта и т.п.).

Чтобы эту инфор­мацию можно было использовать, ее необходимо декодировать с помощью специальных приборов. Примером того, как этот вид носителей защищаемой информации интересует иностранные разведки, могут служить случаи задержания разведчиков и агентов спецслужб на границе с пробами воды, грунта, растений и др.

**5. Электромагнитные, тепловые, радиационные и другие излучения как носители защищаемой информации.**

Радио- и электромагнитные излучения различной частоты переносят информацию от источника информации (радиопере­датчика, излучателя) к приемнику и являются «продуктом» рабо­ты радиотехнических и других систем, и, следовательно, несут информацию об этих системах. Радио- и электромагнитные излуче­ния могут переносить и конфиденциальную, и секретную инфор­мацию. Их распространение, как правило, неконтролируемо и может перехватываться соперником. Для их приема необходимы соответствующие технические приспособления и приборы. О том, что данная перехваченная информация является секретной, может определить только специалист. Для возможного использования такая информация должна быть предварительно декодирована.

**Литература**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
4. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
5. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция № 12**

**Источники, виды и способы дестабилизирующего воздействия**

**на защищаемую информацию**

1. Состав и характеристика источников дестабилизирующего воздействия на защищаемую информацию.

2. Виды и способы дестабилизирующего воздействия на защищаемую информацию.

3. Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на защищаемую информацию.

4. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны людей.

5. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны других источников воздействия.

 **1. Состав и характеристика источников дестабилизирующего воздействия на защищаемую информацию**

Что касается состава структурных частей угро­зы, то необходимо подчеркнуть: **стержневыми, ис­ходными являются источники дестабилизирующе­го воздействия на информацию, от их состава зави­сят и виды, и способы, и конечный результат воз­действия.** Хотя состав других структурных частей угрозы также играет существенную роль, он, в от­личие от источников, не носит определяющего ха­рактера и прямо зависит от источников. Вместе с тем еще раз следует отметить, что источники сами по себе не являются угрозой, если от них не проис­ходит тех или других воздействий.

**К источникам дестабилизирующего воздей­ствия на информацию относятся:**

1. Люди.
2. Технические средства отображения (фикса­ции), хранения, обработки, воспроизведения, пе­редачи информации, средства связи.
3. Системы обеспечения функционирования технических средств отображения, хранения, обра­ботки, воспроизведения и передачи информации.
4. Технологические процессы отдельных кате­горий промышленных объектов.
5. Природные явления.

 **Первый источник -** **люди.** Самым распространенным, многообразным и опасным источником дестабилизирующего воздей­ствия на защищаемую информацию являются люди. Самым распространенным этот источник яв­ляется потому, что дестабилизирующее воздей­ствие на защищаемую информацию могут оказы­вать различные категории людей, как работаю­щих, так и не работающих на предприятии. К ним относятся:

* сотрудники данного предприятия;
* лица, не работающие на предприятии, но име­ющие доступ к защищаемой информации предпри­ятия в силу служебного положения (из вышестоя­щих, смежных (в т.ч. посреднических) предприятий, контролирующих органов государственной и муниципальной власти и др.);
* сотрудники государственных органов развед­ки других стран и разведывательных служб конкурирующих отечественных и зарубежных предпри­ятий;
* лица из криминальных структур, хакеры.

В части соотношения с видами и способами де­стабилизирующего воздействия на информацию эти категории людей подразделяются на две группы:

* имеющие доступ к носителям данной защища­емой информации, техническим средствам ее ото­бражения, хранения, обработки, воспроизведения, передачи и системам обеспечения их функциони­рования и
* не имеющие такового.

Отличия в конкретно применяемых видах и ме­тодах дестабилизирующего воздействия на инфор­мацию между названными группами людей (при однотипности видов и методов) обусловлены пре­следуемыми целями.

Основной целью **второй группы** людей является несанкционированное получе­ние (хищение) информации, являющейся конфи­денциальной. Уничтожение, искажение, блокиро­вание информации стоит на втором плане, а не­редко и не являются целью. Дестабилизирующее воздействие со стороны этой группы людей в по­давляющем большинстве случаев является предна­меренным (умышленным, сознательным). К тому же, для того чтобы осуществить дестабилизирую­щее воздействие на конфиденциальную информа­цию, людям, входящим в эту группу, нужно иметь канал несанкционированного доступа к ней.

Для **первой группы** людей несанкционирован­ное получение конфиденциальной информации во­обще не является целью в силу наличия у них дос­тупа к такой информации. Целями дестабилизиру­ющего воздействия со стороны этой группы явля­ются разглашение, несанкционированное уничто­жение, блокирование, искажение информации (пе­речислены в последовательности, соответствую­щей степени интенсивности воздействия, от боль­шей к меньшей). Хищение информации также при­суще для данной группы, но оно является не це­лью, а средством для осуществления уничтожения или разглашения информации. Предметом воздей­ствия со стороны этой группы является не только конфиденциальная информация (хотя она в первую очередь), но и защищаемая часть открытой инфор­мации. Воздействие со стороны людей, включен­ных в данную группу, может быть:

* как преднаме­ренным,
* так и непреднамеренным (ошибочным, случайным).

Следует, однако, оговориться, что по объектам доступа эта группа неоднородна по сво­ему составу. В нее входят:

1. люди, имеющие доступ и к носителям защищаемой информации, и к сред­ствам отображения, хранения, обработки, воспро­изведения и передачи информации (ко всем или части из них), и к системам обеспечения функцио­нирования этих средств;
2. люди, имеющие доступ только к информации и (иногда или) к средствам ее обработки (всем либо отдельным);
3. люди, допущен­ные только системам обеспечения функционирования средств.

Самым многообразным этот источник являет­ся потому, что ему, по сравнению с другими ис­точниками, присуще значительно большее количе­ство видов и способов дестабилизирующего воз­действия на информацию.

Самым опасным этот источник является пото­му, что:

**во-первых**, он самый массовый,

**во-вторых,** воздействие с его стороны носит не эпизодичес­кий, а регулярный характер,

**в третьих,** как уже от­мечалось, его воздействие может быть не только непреднамеренным, как со стороны других источ­ников, но и преднамеренным, и,

**в-четвертых,** ока­зываемое им воздействие может привести ко всем формам проявления уязвимости информации (со стороны остальных источников - к отдельным фор­мам).

В качестве источников дестаби­лизирующего воздействия на информацию рас­смотрим людей, имеющих доступ к носителям защищаемой информации, техническим средствам ее отображения, хранения, обработки, воспроизведения, передачи и системам обеспече­ния функционирования этих средств, без выше­приведенного разделения этих людей по объектам доступа, поскольку виды и способы дестабилизи­рующего воздействия со стороны различных кате­горий входящих в эту группу людей различаются не составом, а только количеством. Люди, не имеющие, доступ к перечисленным объектам, дестабилизирующее воздействие на ин­формацию могут оказывать, как было отмечено, при наличии каналов несанкционированного дос­тупа к ней.

В зависимости от источника и вида воздействия оно может быть непосредственным на защищае­мую информацию либо опосредованным, через другой источник воздействия.

 **Второй источник** **- технические средства отображения, хране­ния, обработки, воспроизведения, передачи информации и средства связи.**.

К этому источнику относятся:

 - электронно-вычислительная техника;

* электрические и автоматические пишущие ма­шинки и копировально-множительная техника;
* средства видео- и звукозаписывающей и вос­производящей техники;

- средства телефонной, телеграфной, факси­мильной, громкоговорящей передачи информации;

- средства радиовещания и телевидения;

 -средства радио и кабельной связи.

**Третий источник** дестабилизирующего воздействия на информацию - **Системы обеспечения функционирования технических средств отображения, хранения, обра­ботки, воспроизведения и передачи информации:**

системы электро­снабжения,

водоснабжения,

теплоснабжения,

кон­диционирования,

вспомогательные электрические и радиоэлектрон­ные средства (электрические часы, бытовые магнитофоны, радиоприемники, телевизоры и др.)

**Четвертый источник** - **технологические процессы объектов ядерной энергетики, хи­мической промышленности, радиоэлектроники, а также объектов по изготовлению некоторых видов вооружения и военной техники**, которые изменя­ют естественную структуру окружающей объект среды.

 **Пятый источник** **- природные явления** - включа­ет две составляющие:

* стихийные бедствия и
* атмос­ферные явления.

**2. Виды и способы дестабилизирующего воздействия на защищаемую информацию**

Виды и способы дестабилизирующего воздействия на защищаемую информацию дифференцируются по источникам воздействия. Самое большее количество видов и способов дестабилизирующего имеет отношение к людям**.**

**Со стороны людей возможны следующие виды воздействия:**

 1. Непосредственное воздействие на носители за­щищаемой информации.

2.Несанкционированное распространение конфиденциальной информации.

3.Вывод из строя технических средств отобра­жения, хранения, обработки, воспроизведения, пе­редачи информации и средств связи.

4.Нарушение режима работы перечисленных средств и технологии обработки информации.

5.Вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

**Способами непосредственного воздействия** на носители защищаемой информации могут быть:

* физическое разрушение носителя (поломка, разрыв и др.);
* создание аварийных ситуаций для носителей (поджог, искусственное затопление, взрыв и т.д.);
* удаление информации с носителей (замазыва­ние, стирание, обесцвечивание и др.);
* создание искусственных магнитных полей для размагничивания носителей;
* внесение фальсифицированной информации в носители.

Этот вид дестабилизирующего воздействия при­водит к реализации трех форм проявления уязви­мости информации: уничтожению, искажению и блокированию.

К непосредственному воздействию на носите­ли защищаемой информации можно с оговоркой отнести и непреднамеренное оставление их в нео­храняемой зоне, чаще всего в общественном транс­порте, магазине, на рынке, что приводит к потере носителей.

**Несанкционированное распространение конфиденциальной информации может осуществ­ляться путем***:*

* *.* словесной передачи (сообщения) информа­ции;
* передачи копий (снимков) носителей инфор­мации;
* показа носителей информации;
* ввода информации в вычислительные сети;
* опубликования информации в открытой пе­чати;
* использования информации в открытых пуб­личных выступлениях, в т.ч. по радио, телевидению.

К несанкционированному распространению может привести и потеря носителей информации.

Этот вид дестабилизирующего воздействия при­
водит к разглашению конфиденциальной информации.

**К способам вывода из строя технических средств отображения, хранения, обработки, вос­произведения, передачи информации и средств связи можно отнести**:

* неправильный монтаж средств;
* поломку (разрушение) средств, в т.ч. разрыв (повреждение) кабельных линий связей;
* создание аварийных ситуаций для техничес­ких средств (поджог, искусственное затопление, взрыв и др.);
* отключение средств от сетей питания;
* вывод из строя или нарушение режима рабо­ты систем обеспечения функционирования средств;
* вмонтирование в ЭВМ разрушающих радио и программных закладок.

Этот вид дестабилизирующего воздействия при­водит к реализации трех форм проявления уязви­мости информации: уничтожению, искажению и блокированию.

**Способами нарушения режима работы тех­нических средств отображения, хранения, обра­ботки, воспроизведения, передача информации, средств связи и технологии обработки информа­ции могут быть:**

* повреждение отдельных элементов средств;
* нарушение правил эксплуатации средств;
* внесение изменений в порядок обработки ин­формации;

-заражение программ обработки информации вредоносными программами;

* выдача неправильных программных команд;
* превышение расчетного числа запросов;
* создание помех в радио эфире с помощью до­полнительного звукового или шумового фона, из­менения (наложения) частот передачи информа­ции; .

-передача ложных сигналов; ... - подключение подавляющих фильтров в инфор­мационные цепи, цепи питания и заземления;

* нарушение (изменение) режима работы сис­тем обеспечения функционирования средств.
* Данный вид дестабилизирующего воздействия

также приводит к уничтожению, искажению и бло­кированию информации.

**К способам вывода из строя и нарушения ре­жима работы систем обеспечения функциониро­вания технических средств отображения, хране­ния, обработки, воспроизведения и передачи ин­формации следует отнести:**

*-* неправильный монтаж систем;

- поломку (разрушение) систем или их элементов;

* создание аварийных ситуаций для систем (под­жог, искусственное затопление, взрыв и т.д.);
* отключение систем от источников питания;
* нарушение правил эксплуатации систем.

Этот вид дестабилизирующего воздействия при­водит к тем же результатам, что и два предыдущих вида.

К видам дестабилизирующего воздействия на защищаемую информацию со стороны второго источника воздействия - технических средств отображения, хранения, обработки, воспроизве­дения, передачи информации и средств связи относятся:

1.Выход средств из строя.

2.Сбои в работе средств.

3.Создание электромагнитных излучений.

 **Выход средств из строя**, приводящий к невозмож­ности выполнения операций, может происходить путем:

* технической поломки, аварии (без вмешательства людей);
* возгорания, затопления (без вмешательства людей);
* выхода из строя систем обеспечения функцио­нирования средств;
* воздействия природных явлений;
* воздействия измененной структуры окружающего магнитного поля;
* заражения программ обработки информации вредоносными программами (путем размножения последних или с зараженных дискет);
* разрушения или повреждения носителя информации, в том числе размагничивания магнитного слоя диска (ленты) из-за осыпания магнитного порошка.

Этот вид дестабилизирующего воздействия при­водит к реализации трех форм проявления уязви­мости информации: уничтожению, искажению, блокированию.

**Сбои в работе средств, приводящие к непра­вильному выполнению операций (ошибкам), мо­гут осуществляться посредством:**

* возникновения технических неисправностей элементов средств;
* заражения программ обработки информации вредоносными программами (путем размножения последних или с зараженных дискет);

-воздействия природных явлений;

* воздействия окружающего магнитного поля;
* частичного размагничивания магнитного слоя диска (ленты) из-за осыпания магнитного порош­ка;
* нарушения режима функционирования систем обеспечения функционирования средств.

Данный вид дестабилизирующего воздействия приводит к реализации четырех форм проявления уязвимости информации: уничтожению искаже­нию, блокированию, разглашению (пример после­дней - соединение с номером телефона не того або­нента, который набирается, или слышимость раз­говора других лиц из-за неисправности в цепях ком­мутации телефонной станции).

**Электромагнитные излучения**, в том числе побочные, образующиеся в процессе эксплуатации средств, приводят к хищению информации.

Третий источник дестабилизирующего воздей­ствия на информацию - системы обеспечения фун­кционирования технических средств отображе­ния, хранения, обработки, воспроизведения и пе­редачи информации - включает два вида воздей­ствия:

1 .Выход систем из строя.

2.Сбои в работе систем.

**Выход систем из строя** может происходить пу­тем:

* поломки, аварии (без вмешательства людей);
* возгорания, затопления (без вмешательства лю­дей);
* выхода из строя источников питания;
* воздействия природных явлений.

Этот вид дестабилизирующего воздействия при­водит к реализации трех форм проявления уязви­мости информации: уничтожению, блокированию, искажению.

**Сбои в работе систем** могут осуществляться посредством:

*-* появления технических неисправностей эле­ментов систем;

- воздействия природных явлений;

- нарушения режима работы источников питания.

Результатом дестабилизирующего воздействия также являются уничтожение, блокирование, ис­кажение информации.

Видом дестабилизирующего воздействия на информацию со стороны технологических процессов отдельных промышленных объектов являет­ся **изменение структуры окружающей среды**.

Это воздействие осуществляется путем:

*-* изменения естественного радиационного фона окружающей среды, происходящего при функционировании объектов ядерной энергетики;

- изменения химического состава окружающей среды, происходящего при функционировании объектов химической промышленности;

- изменения локальной структуры магнитног поля, происходящего вследствие деятельности объектов радиоэлектроники и по изготовлению некоторых видов вооружения и военной техники. Этот вид дестабилизирующего воздействия в ко­нечном итоге приводит к хищению конфиденци­альной информации.

Пятый источник дестабилизирующего воздей­ствия на информацию - природные явления, как уже отмечалось, включает стихийные бедствия и атмосферные явления (колебания).

К стихийным бедствиям и одновременно видам воздействия следует отнести:

* землетрясение,
* навод­нение,
* ураган (смерч),
* шторм,
* оползни,
* лавины,
* извержения вулканов.

К атмосферным явлениям (видам воздействия) относят:

* грозу,
* дождь,
* снег,
* перепады температуры и влажности воздуха,
* магнитные бури.

Способами воздействия со стороны и стихий­ных бедствий, и атмосферных явлений могут быть:

* разрушение (поломка),
* затопление,
* сожжение но­сителей информации, средств отображения, хра­нения, обработки, воспроизведения, передачи ин­формации и кабельных средств связи, систем обес­печения функционирования этих средств,
* наруше­ние режима работы средств и систем, а также тех­нологии обработки информации.

Эти виды воздействия приводят к пяти формам проявления уязвимости информации: потере, унич­тожению, искажению, блокированию и хищению.

При рассмотрении признаков и составляющих угрозы защищаемой информации было сказано, что в основе любого дестабилизирующего воздей­ствия лежат определенные причины, побудитель­ные мотивы, которые обусловливают появление того или другого вида и способа воздействия. Вме­сте с тем и причины имеют под собой основания - обстоятельства или предпосылки, которые вызы­вают данные причины, способствуют их появле­нию. Однако наличие источников, видов, способов, причин и обстоятельств (предпосылок) дестабили­зирующего воздействия на информацию представ­ляет потенциально существующую опасность, ко­торая может быть реализована только при наличии определенных условий для этого.

Поскольку виды и способы дестабилизирующе­го воздействия зависят от источников воздействия, то и причины, обстоятельства (предпосылки) и ус­ловия должны быть привязаны к источникам воз­действия.

**3. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны людей.**

Применительно к людям причины, обстоятель­ства и условия в большинстве случаев увязаны еще и с характером воздействия - преднамеренным или непреднамеренным.

К причинам, вызывающим преднамеренное дес­табилизирующее воздействие, следует отнести:

* стремление получить материальную выгоду (подзаработать);
* стремление нанести вред (отомстить) руковод­ству или коллеге по работе, а иногда и государству;
* стремление оказать бескорыстную услугу при­ятелю из конкурирующей фирмы;
* стремление продвинуться по службе;
* стремление обезопасить себя, родных и близ­ких от угроз, шантажа, насилия;
* физическое воздействие (побои, пытки) со сто­роны злоумышленника;
* стремление показать свою значимость.

Обстоятельствами (предпосылками), способствующими появлению этих причин, могут быть:

* тяжелое материальное положение, финансовые затруднения;
* корыстолюбие, алчность;
* склонность к развлечениям, пьянству, наркоти­кам;
* зависть, обида;
* недовольство политикой государства, предприятия, политическое или на­учное инакомыслие;
* личные связи с представителями конкурента;
* недовольство служебным положением, карье­ризм;
* трусость, страх;
* тщеславие, самомнение, завышенная само­оценка, хвастовство.

К условиям, создающим возможность для дес­табилизирующего воздействия на информацию, можно отнести:

* недостаточность мер, принимаемых для защи­ты информации, в том числе из-за нехватки ресур­сов;
* недостаточный контроль и внимание со сторо­ны администрации вопросам защиты, информа­ции;
* принятие решений по производственным воп­росам без учета требований по защите информа­ции;
* плохие взаимоотношения между сотрудника­ми и сотрудников с администрацией.
* Причинами непреднамеренного дестабилизиру­ющего воздействия на информацию со стороны людей могут быть:
* неквалифицированное выполнение операций;
* халатность, безответственность, недисциплини­рованность, недобросовестное отношение к выпол­няемой работе;
* небрежность, неосторожность, неаккуратность;
* физическое недомогание (болезни, переутом­ление, стресс, апатия).

К обстоятельствам (предпосылкам) появления этих причин можно отнести:

* низкий уровень профессиональной подготов­ки;
* излишняя болтливость, легкомыслие, привычка делиться опытом, давать советы;
* незаинтересованность в работе (вид работы, своевременный характер, зарплата), отсутствие стимулов для ее совершенствования;
* разочарованность в своих возможностях и спо­собностях;
* перегруженность работой, срочность ее выпол­нения, нарушение режима работы;
* плохое отношение со стороны администрации.

Условиями для реализации непреднамеренного дестабилизирующего воздействия на инфор­мацию могут быть:

* отсутствие или низкое качество правил ра­боты с защищаемой информацией;
* незнание или нарушение правил работы с ин­формацией исполнителями;
* недостаточный контроль со стороны админист­рации за соблюдением режима конфиденциально­сти;
* недостаточное внимание со стороны админис­трации условиям работы, профилактике заболева­ний, повышению квалификации.

**4. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны других источников воздействия.**

Причинами дестабилизирующего воздействия на информацию со стороны технических средств отображения, хранения, обработки воспроизведения, передачи информации и средств связи могут быть:

* недостаток или плохое качество средств;
* низкое качество режима функционирования средств;
* перезагруженность средств;
* низкое качество технологии выполнения работ;
* дестабилизирующее воздействие на средства со стороны других источников воздействия.

К обстоятельствам (предпосылкам), вызываю­щим эти причины, следует отнести:

недостаточность финансовых ресурсов, выде­ляемых на приобретение и эксплуатацию средств;

плохой выбор средств;

старение (износ) средств;

конструктивные недоработки или ошибки при монтаже средств;

-ошибки при разработке технологии выполнения работ, в том числе программного обеспечения;

дефекты используемых материалов;

чрезмерный объем обрабатываемой информа­ции;

причины, лежащие в основе дестабилизирую­щего воздействия на средства со стороны других источников воздействия.

Условиями, обеспечивающими реализацию дес­табилизирующего воздействия на информацию со стороны технических средств, могут являться:

- недостаточное внимание к составу и качеству средств со стороны администрации, нередко из-за недопонимание их значения;

- нерегулярный профилактический осмотр средств;

- низкое качество обслуживания средств.

Причины, обстоятельства (предпосылки) и усло­вия дестабилизирующего воздействия на инфор­мацию со стороны систем обеспечения функцио­нирования средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи «вписываются» в причины и обстоя­тельства воздействия со стороны самих средств.

Причиной дестабилизирующего воздействия на информацию со стороны технологических процес­сов отдельных промышленных объектов является специфика технологии, обстоятельством - необхо­димость такой технологии, а условием - отсутствие возможностей противодействия изменению струк­туры окружающей среды.

В основе дестабилизирующего воздействия на информацию со стороны природных явлений ле­жат внутренние причины и обстоятельства, непод­контрольные людям, а следовательно, и не поддаю­щиеся нейтрализации или устранению.

 Следует заметить, что не всегда можно провести грань между причинами и обстоятельствами, один и тот же фактор в одном случае может быть причи­ной, в другом обстоятельством (предпосылкой), виды дестабилизирующего воздействия со сторо­ны одних источников могут выступать в роли спо­собов дестабилизирующего воздействия со сторо­ны других источников. ­

**Литература**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
4. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
5. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция № 13**

**Назначение и структура систем защиты информации**

1. Понятия «системный подход» и «система».

2. Требования к системе защиты информации.

3. Структура системы защиты информации.

4. Понятие комплексной системы защиты информации на предприятии как формы организации деятельности по защите информации.

.5. Оценка эффективности КСЗИ.

**1. Понятия «системный подход» и «система»**

Общая теория защиты секретов является составной и неразрывной частью теории обеспечения национальной безопас­ности государства, укрепления его обороноспособности и эконо­мической мощи. Защита информации охватывает и вовлекает в свою орбиту различные структуры государственного аппарата, ор­ганы и предприятия независимо от форм их собственности, орга­низации и фирмы и т.д. Все эти структуры государства связаны друг с другом, причем не какими–то случайными связями, а ус­тойчивыми, влияющими друг на друга и зависящими друг от друга. Разобраться во всем многообразии этих связей можно только тогда, когда мы применим для рассмотрения проблем защиты информации системный подход.

**Под системным подходом** понимается методологическое на­правление в науке, основная задача которого состоит в разработке методов исследования и конструирования сложноорганизованных объектов — систем разного типа и классов. Системный под­ход используется в целях познания, исследовательской и кон­структорской деятельности, описания и объяснения природы ана­лизируемых или искусственно создаваемых объектов1. Под систе­мой же обычно понимают совокупность элементов, находящихся в отношениях и связях между собой и образующих определенную целостность, единство.

Системный подход к исследованию проблем защиты инфор­мации позволит проще взглянуть на все сложные свя­зи системы защиты информации со всеми другими системами, с внешней средой, выявить и понять сущность деятельности по за­щите информации. Однако следует осознать, что защита информации имеет самостоятельное значение лишь относитель­но. Она призвана обеспечить нормальное и эффективное функ­ционирование вышестоящей системы, в которую она «встроена» и которой она создана: например, обеспечивать деятельность от­расли, предприятия, фирмы и т.д. Цель режимной деятельности на любом предприятии состоит в том, чтобы обеспечить научно–производственную, управленческую и другую деятельность сек­ретной и другой защищаемой информацией. Поэтому система за­щиты информации является системой режимного информацион­ного обслуживания другой системы, являющейся по отношению к ней вышестоящей.

**2. Требования к системе защиты информации**

Любая система за­щиты информации имеет свои особенности и в то же время долж­на отвечать общим требованиям. Наиболее общими требования­ми к системе защиты информации являются следующие.

1. Система защиты информации должна быть пред­ставлена как нечто целое. **Целостность** системы будет выражаться в наличии: единой цели ее функционирования, информационных связей между элементами системы, иерархичность построения подсистемы управления системой защиты информации. Ни одна ее часть не может быть изъята без ущерба для всей системы..
2. Система защиты информации должна обеспечивать:
* безопасность информации,
* средств информации и
* защиту инте­ресов участников информационных отношений.
1. Система защиты информации должна обеспечи­вать **информационные связи** внутри системы между ее элемента­ми, обеспечивающие их согласованное функционирование, и связи с внешней средой, перед которой система проявляет свою целостность и выступает как единое целое.
2. Система защиты информации должна охватывать весь **технологический комплекс** информационной деятельности.
3. Система защиты информации быть **разнообразной** по используемым средствам, многоуровневой с иерархической последовательностью доступа.
4. Система защиты информации должна быть **открытой** для изменения и дополнения мер обеспечения безопасности информации.
5. Система защиты информации должна быть **нестандартной**. При выборе средств защиты нельзя рассчитывать на неосведомленность злоумышленников относительно ее возможностей.
6. Система защиты информации должна быть **простой** для технического обслуживания и **удобной** для эксплуатации пользователями.
7. Система защиты информации должна быть **надежной.** Любые поломки технических средств являются причиной появления неконтролируемых каналов утечки информации.

**3. Структура системы защиты информации**

**С одной стороны,** система защиты информации включает в себя совокупность элементов ее образующих и их свойства. Внут­ренние связи системы и их свойства составляют архитектуру сис­темы, ее структуру и внутреннюю организацию.

**С другой стороны,** элементы системы имеют внешние связи, которые целенаправ­ленно воздействуют на внешнюю среду и решают поставленные перед системой задачи. Это есть функциональная часть системы. Вполне естественно, что эти две. части, две стороны — функцио­нальная и структурная — не отделены друг от друга, это как бы две стороны одних и тех же элементов, составляющих систему защиты информации.

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

**Структурная часть системы защиты информации включает в себя:**

1. **Систему законов и других нормативных актов,** устанавливающих:
* порядок и правила защиты информации, а также ответст­венность за покушение на защищаемую информацию или на ус­тановленный порядок ее защиты;
* защиту прав граждан, связанных по службе со сведениями,
отнесенными к охраняемой тайне;
* права и обязанности государственных органов, предприятий
и должностных лиц в области защиты информации.

**2. Систему засекречивания информации**, включающую:

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

**3. Систему режимных служб и служб безопасности** с их собственной структурой, штатным расписанием, обеспечивающих
функционирование всей системы защиты информации.

Структурная часть системы защиты информации является ус­тойчивой частью данной системы, ее консервативной частью. Как видно из перечисления основных элементов структурной части системы, ее элементы могут изменяться только «скачкообразно», они не могут приспосабливаться быстро и непрерывно в связи с изменениями внешней среды, а также изменениями обстановки, поскольку внешняя среда может оказывать влияние на структур­ную часть системы защиты информации лишь через ее функцио­нальную часть, то есть опосредованно.

Положительная сторона устойчивости и консерватизма этой части системы заключается в том, что она оказывается своеобраз­ным фильтром, отбраковывающим те реакции системы на изме­нение внешней среды, которые являются недостаточно обоснованными и мотивированными со стороны потребностей общест­ва.

Недостатками консерватизма системы защиты информации является то, что эта часть системы может часто иметь рассогласо­вания и противоречия с ее функциональной частью. Это, естест­венно, сказывается на эффективности и оптимальности функци­онирования системы защити информации.

**Функциональная часть системы защиты информации** решает задачи обеспечения засекреченной информацией деятельности вышестоящей системы, в которую данная система защиты инфор­мации «встроена» (предприятие, фирма и т.д.). В эту деятельность вовлекается широкий круг работников объекта: сотрудники служ­бы безопасности, связанные с обработкой, хранением, выдачей и учетом засекреченной информации; руководители объекта и структурных подразделений; исполнители, тесть все работники объекта, которые являются потребителями защищаемой инфор­мации.

Эта часть системы защиты информации более адаптивна, по­движна и пластична. Она, исполняя свое предназначение, макси­мально стремится учесть потребности внешней среды в решении вопросов обращения и циркулирования защищаемой информа­ции, обеспечение ею потребителей и в то же время – исключить выход ее за пределы охраняемой сферы, ее разглашение или рас­крытие.

**Основные элементами функциональной части системы:**

* порядок и правила **засекречивания (**определения степени секретности сведений и проставление грифа секретности на работах, документах, изделиях) и **рассекречивания** информации или снижения степени ее секретности;
* установленные на объекте **режим секретности**, внутри–объектовый режим и режим охраны, соответствующие важности накапливаемой и используемой на объекте информации;
* **система обработки, хранения, учета и выдачи носителей за­щищаемой информации** с использованием принятой системы на­копления и обработки информации: автоматизированная, ручная, смешанная, иная, в том числе делопроизводство с секретными и конфиденциальными документами;
* **разрешительная система**, регламентирующая порядок досту­па потребителей к носителям защищаемой информации, а также
на предприятие и в его отдельные помещения;
* **система выявления возможных каналов утечки защищаемой
информации** и поиск решений по их перекрытию, включая вос­питательно–профилактическую работу на объекте и в его струк­турных подразделениях;
* **система** контроля наличия носителей защищаемой инфор­мации и состояния на объекте установленных режимов: секрет­ности, внутриобъектового, охраны объекта и его важнейших подразделений.

Таким образом, можно сказать, что и структурная и функцио­нальная части системы защиты информации существуют и рабо­тают в неразрывном единстве.

**4. Понятие комплексной системы защиты информации на предприятии как формы организации деятельности по защите информации.**

Система защиты информации на предприятии носит, как пра­вило, комплексный характер. Это обусловливается характером на­капливаемой и используемой предприятием защищаемой инфор­мации, вовлечением большого числа сотрудников в работу с за­секреченной информацией, разнообразием носителей, на кото­рых она накапливается, высокой подвижностью информацион­ных процессов. Такая система создается с учетом и в рамках при­нятых концепции и стратегии защиты информации.

**Комплексная система защиты информации (КСЗИ)** — это со­вокупность сил, средств, методов и мероприятий, используемых во взаимодействии и дополнении друг друга и предназначенных для обеспечения на регулярной основе и на заданном уровне за­щиты информации на этом объекте.

**Конкретизация объекта, предмета, целей и задач защиты ин­формации на предприятии.**

На каждом предприятии накапливаются и используются зна­чительные объемы информации различных категорий и разной степени важности. Какая–то часть наиболее важной информации, принадлежащей государству или предприятию, может засекречи­ваться и объявляться государственной или коммерческой тайной. В зависимости от характера производства, выпускаемой продук­ции, используемых технологий, ведущихся НИОКР, связей со смежниками, поставщиками и потребителями продукции решает­ся вопрос об отнесении имеющейся, вновь создаваемой и полу­чаемой информации к сведениям, составляющим государственную или коммерческую тайну.

Таким образом, происходит разде­ление информации на массивы: массив открытой информации, массив информации, являющейся государственной тайной, и массив информации, отнесенной к коммерческой тайне. Послед­ние два массива информации и являются объектом защиты ре­жимных служб предприятия.

Следует различать **объект и предмет защиты информации.**

**Объектом защиты информации** являются различные категории сведений, имеющихся на данном предприятии, и отнесенные в соот­ветствии с установленными законодательными и другими норматив­ными актами к составляющим государственную или коммерческую тайну. Соперника могут интересовать военно–промышленные пред­приятия, средства вооружения и технологии, научно–технические ре­шения. При наличии возможностей соперник может попытаться по­лучить к ним доступ и путем непосредственного наблюдения и ис­пользования технических средств получить о них информацию. Однако он может получить доступ и к информации, отображающей сведения об интересующих его объектах разведки. Порой бывает проще получить доступ к носителям информации об объектах раз­ведки, чем к самим объектам, и кроме того, носители могут содер­жать более полную информацию об интересующих его вопросах, чем он сможет получить путем непосредственного наблюдения.

Таким образом, объекты защиты информации на предприятии – это 1) сами объекты разведки (новейшие виды воору­жения, военной техники, технологии, ноу–хау и др.), являющиеся носителями защищаемой информации, 2) сведения о них, от­несенные к государственной или коммерческой тайне, используе­мые и хранящиеся на данном предприятии, и к которым прояв­ляет или может проявить интерес соперник.

**Предметом** защиты информации являются носители информа­ции, на которых зафиксированы, отображены защищаемые све­дения: секретные документы; специзделия; материалы; излуче­ния, несущие и отображающие защищаемую информацию.

Если объект защиты выглядит несколько абстрактно — госу­дарственная или коммерческая тайна, то предмет защиты, как правило, материализован в виде документа, изделия, материала, или отображается в виде знания в памяти и сознании человека, осведомленного в сведениях, составляющих охраняемую тайну. Именно на охрану предмета — носителей засекреченной инфор­мации — и направлены главным образом усилия работников ре­жимных служб и служб безопасности.

**Цели и задачи защиты информации на предприятии**. Постро­ение любой системы начинается с определения целей и задач

функционирования создаваемой системы защиты информации. Наиболее общими ее **задачами** на предприятии будут следующие:

1. Обеспечить научно–производственную, управленческую, фи­нансовую, хозяйственную, маркетинговую и иную деятельность предприятия режимным информационным обслуживанием, то есть снабжением всех служб, подразделений и должностных лиц необхо­димой информацией, как засекреченной, так и несекретной. При этом деятельность по защите информации по возможности не должна создавать больших помех и неудобств в решении производственных и прочих задач, и в то же время способствовать их эффективному решению, давать предприятию преимущества перед конкурентами и оправдывать затраты средств на защиту информации.
2. Гарантировать безопасность информации, ее средств, предотвратить утечку защищаемой информации и предупредить любой несанкционированный доступ к носителям засекреченной информации.
3. Создать условия и возможности для коммерческого использования секретной и конфиденциальной информации предпри­ятия. Это прежде всего технологической информации, содержа­щей ноу–хау, так как излишнее ее перехранение может привести к ее старению и обесцениванию.
4. Документировать процесс защиты информации, особенно сведений, составляющих коммерческую тайну с тем, чтобы в слу­чае возникновения необходимости обращения в правоохранительные органы, иметь соответствующие доказательства, что предпри­ятие принимало необходимые меры к защите этих сведений.

Эта система должна решать вполне определенный круг задач: обеспечивать бесперебойное снабжение деятельности предпри­ятия необходимой информацией, как засекреченной, так и несек­ретной, обеспечивать защиту от соперника секретной и конфи­денциальной информации.

Одним из этапов построения КСЗИ **является подготовка методи­ческих организационно–правовых документов.** Для достижения по­ставленных перед КСЗИ целей и согласованных действий всех под­разделений и должностных лиц предприятия разрабатываются мето­дические организационно–правовые документы, регламентирующие режимные меры, обеспечивающие обращение защищаемой инфор­мации в заданной сфере, ее безопасность и недоступность незаконно­му потребителю. В этих документах должна находить воплощение идея комплексного подхода к защите информации на предприятии. Основные из этих документов мы рассматривали выше (см.: Защита коммерческой тайны), однако учитывая, что на предприятии могут одновременно проводиться работы, связанные с использованием сведений, составляющих как государственную тайну, так и коммер­ческую тайну, следует дополнительно дать несколько пояснений.

**Во–первых,** в Уставе должно быть указано, что данное пред­приятие имеет право проводить работы с использованием сведе­ний, составляющих государственную тайну, наличие лицензии на право проведения работ со сведениями соответствующей степени секретности. Предприятие имеет право создавать у себя специаль­ные службы, обеспечивающие защиту информации2.

**Во–вторых,** предприятие может иметь как минимум два пере­чня сведений, подлежащих засекречиванию: отраслевой или уточ­ненный для данного предприятия Перечень сведений, составля­ющих государственную тайну, и подготовленный специалистами предприятия Перечень сведений, составляющих коммерческую тайну предприятия.

**В–третьих,** иметь на предприятии две инструкции, регламенти­рующие: одна — порядок и правила защиты сведений, составля­ющих государственную тайну, другая — коммерческую тайну.

**В–четвертых,** на предприятии может быть подготовлено не­сколько положений, регламентирующих как деятельность отдель­ных подразделений, выполняющих функции по защите информа­ции (СБ, подразделение противодействия ТСР и др.), так и уста­навливающих порядок решения определенных вопросов, напри­мер, о порядке подготовки материалов, предназначенных к опуб­ликованию в открытой печати.

В методических организационно–правовых документах, осо­бенно в инструкциях и положениях, следует указать использование в защите информации методов и средств, которыми располагает предприятие. Например, метод ранжирования, который следует указывать не вообще, а как конкретно используется этот метод. Показать также, что информация делится по степени секретности и конфиденциальности, кто имеет право давать разрешение на до­пуск к той или иной степени секретности информации.

Рассматривая в методологическом аспекте проблему создания КСЗИ следует еще раз обратиться к факторам, при наличии ко­торых происходит или может происходить утечка информации. Она может произойти, если: 1) на предприятии имеется инфор­мация, интересующая соперника; 2) имеется соперник, который заинтересован в добывании этой информации и прилагает для этого усилия и активность; и 3) канал утечки информации, то есть возможность или способы несанкционированного доступа сопер­ника к защищаемым носителям информации, при этом со сторо­ны защитников и пользователей этой информацией допускаются отступления от правил защиты информации, чему способствуют и складывающиеся неблагоприятные условия.

Обращение к этой схеме подсказывает логику рассуждений при решении проблем построения систем защиты информации. Из схемы мы можем определить, на какие элементы данной сис­темы — канала утечки информации — предприятие может воз­действовать своими силами и средствами, с помощью каких ме­тодов и средств, чтобы предупредить утечку информации. Оказы­вается, что предприятие может воздействовать:

* на носители защи­щаемой информации — возможные потенциальные источники утечки информации;
* на условия, которые не благоприятствуют защите информации; на причины утечки информации, если они появляются по вине предприятия и работающих на нем лиц.
* На соперника, стремящегося добыть секретную и конфиден­циальную информацию, и используемые им для несанкционированного доступа к этой информации силы и средства, предпри­ятие, как правило, воздействовать не может.

Отсюда просматриваются **общеметодологические подходы к построению КСЗИ:**

а) создать условия, обеспечивающие непрерывность защиты
носителей секретной или конфиденциальной информации, при­
чем не только в местах их хранения, но и, главным образом, когда
информация находится в движении, то есть когда она обрабаты­вается, передается, пересылается и используется, когда информа­ция «живет» и работает;

б) постоянно работать с людьми в двух основных направлени­ях: во–первых, чтобы сотрудники, осведомленные в секретных или конфиденциальных сведениях, сами не явились источниками утечки этих сведений путем их разглашения; во–вторых, чтобы
они строго выполняли правила защиты носителей засекреченной
информации и не явились причиной получения несанкциониро­ванного доступа к ним соперника, или не создавали благоприят­ных для этого условий.

 Разведка соперника, как правило, изучает все носители инте­ресующей его информации и отыскивает среди них наиболее уяз­вимые («слабое звено»). Именно недостаточная надежность само­го носителя (человека) или его защиты (любого другого матери­ального носителя засекреченной информации) создают потенци­альную возможность несанкционированного доступа к этой ин­формации и ее утечки. С учетом этого возможные источники утечки защищаемой информации можно разделить на три группы:

* люди, хранящие секретную или конфиденциальную инфор­мацию в своей памяти;
* документы, изделия, материалы или другие носители, ото­браженная на которых или в которых информация находится в относительно статическом состоянии;
* излучения, колебания и другие физические процессы, пере­дающие («переносящие») информацию. Информация находится в динамике, причем, иногда очень краткосрочно.

Исходя из рассмотрения групп носителей защищаемой инфор­мации – возможных потенциальных источников утечки инфор­мации – следует намечать меры защиты засекреченной информа­ции на предприятии.

**Первая группа носителей защищаемой информации** это люди – основные меры и методы защиты секретной или конфи­денциальной информации в памяти этих носителей всегда носят интеллектуальный характер:

* подбор людей, допускаемых к секретным работам, их проверка и изучение;
* обучение лиц, допущенных к секретам, правилам их сохранения;
* воспитание секретонсителей пониманию важности сохране­ния в тайне доверенных им секретных или конфиденциальных сведений; стимулирование заинтересованности работы с засекре­ченной информацией и сохранения этих сведений в тайне; угроза ответственности и серьезных последствий для них за несохране­ние в тайне по их вине доверенных им секретов и т.д.;
* иные меры: добровольное согласие на ограничение прав чело­века, допускаемого к работе с засекреченной информацией, в частности, нельзя работать по совместительству у конкурентов, вступать без служебной необходимости в контакты с иностранца­ми, ограничения на выезд и возможные служебные командировки за границу и др.;
* дробление (расчленение) информации о технологических про­цессах на операции, знание одной из которых не дает возмож­ность восстановить весь технологический процесс;
* строгое ранжирование секретной или конфиденциальной ин­формации по ее важности и доступа к ней пользователей. **Вторая группа носителей защищаемой информации** – матери­альные носители, которые могут стать источником информации только в том случае, если соперник, злоумышленник незаконно получит к ним непосредственный доступ. Основные методы за­щиты секретной или конфиденциальной информации, отражен­ной на подобных носителях:
* учет всех носителей защищаемой информации;
* персональная ответственность за сохранность каждого носите­ля такой информации;
* ранжирование секретной и конфиденциальной информации по уровням секретности и в соответствии с этим – регламентация доступа к ней;
* контроль за использованием носителей защищаемой информа­ции;
* физическая охрана носителей защищаемой информации с ис­пользованием технических средств, и др.

**Третья группа носителей** секретной и конфиденциальной ин­формации. «Снятие», получение информации с этих носителей возможно только с использованием специальной аппаратуры, а ее декодирование – специалистами, располагающими определен­ным минимумом предварительных знаний (за сравнительно ред­ким исключением, когда по открытым каналам связи ведутся раз­говоры на «закрытые» темы открытым текстом).

Основные методы, защиты секретной и конфиденциальной ин­формации, «переносимой» указанными носителями информации:

* скрытие;
* дезинформация;
* кодирование и шифрование, а также организационные и
инженерно–технические меры.

Все названные группы средств и методов защиты информации применяются в рамках действующих законов, инструкций и дру­гих нормативных актов. Они должны предусматриваться в разра­батываемых на предприятии нормативных документах по органи­зации защиты информации.

**5. Оценка эффективности КСЗИ.**

Постоянный контроль за движением и наличием секретных и конфиденциальных документов, специзделий и подобных мате­риалов, за соблюдением всеми исполнителями и работниками служб безопасности правил и порядка защиты информации со­провождается, или, во всяком случае, должен сопровождаться, оценкой эффективности функционирования КСЗИ.

Оценка эффективности систем защиты информации – пробле­ма комплексная, многокритериальная, требующая рассмотрения многих факторов, влияющих на функционирование этой системы.

**Во-первых,** оценка эффективности СЗИ является управлен­ческой функцией, как бы завершающей управленческий цикл.

**Во-вторых,** данную задачу следует рассматривать на двух уров­нях управления: на стратегическом и тактическом.

**В-третьих,** оценку эффективности СЗИ следует проводить в рамках всей иерархии систем.

**В-четвертых,** оценка эффективности может быть более или менее точно проведена, если четко сформулированы цели дея­тельности СЗИ.

И тогда оценка эффективности КСЗИ будет состоять в про­верке соответствия достижения какой-то конкретной системой целей, которые ей были определены при ее создании или на оче­редном этапе ее функционирования.

Цели защиты информации должны вытекать из целей деятель­ности предприятия, учреждения, организации, то есть системы более высокого уровня, в рамках которой функционирует КСЗИ. Поэтому ее эффективность следует рассматривать как функцию системы более высокого порядка, так как она предназначена спо­собствовать эффективному функционированию этой системы и всех других систем, зависящих от эффективности функциониро­вания данной КСЗИ.

Конкретная система должна также рассматриваться в связи, в «комплекте» с другими системами, в которых имеются те же секре­ты, которые охраняет рассматриваемая («наша») система. Сопер­нику ведь не обязательно одну и ту же информацию добывать в каждом месте, где она имеется. Если он интересующую его инфор­мацию получил там, где она сохранялась не очень тщательно, он уже не будет стремиться получить ее в других местах. Поэтому, хотя наша система сработала, допустим, хорошо, сохранила секреты от утечки, цель таким образом для нас вроде бы достигнута, однако, если посмотреть с точки зрения систем более высокого порядка, то безусловно — нет. Следовательно, оценка эффективности СЗИ с точки зрения достижения **стратегических целей** может произво­диться только по «конечному результату», в координатах систем более высокого порядка, в комплексес другими системами.

Когда рассматривается эффективность КСЗИ **на тактическом уровне,** то учитывается уже только функционирование данной системы в Целом, а также отдельных ее элементов (подсистем). Оценивается деятельность по защите информации каждого под­разделения, каждого сотрудника с точки зрения соблюдения пра­вил сохранения в тайне засекреченной информации, не создавали ли они условия, которые могли бы способствовать или привести к утечке информации, или создать иные угрозы ее безопасности.

В то же время каждый без труда может увидеть, что тактичес­кий и стратегический уровни оценки эффективности КСЗИ на­ходятся в тесной взаимосвязи, в прямой зависимости: нарушения режима секретности и другие недостатки в организации защиты засекреченной информации, приведшие к ее утечке, есть не что иное, как недостаточная эффективность систем защиты инфор­мации на тактическом уровне, ущерб же сказывается на всех уров­нях, в том числе, естественно, и на стратегическом.

**Литература**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
4. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
5. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция № 4**

**ЗАЩИТА ИНФОРМАЦИИ В ИС**

1. Цели защиты и виды угроз

2. Методы защиты информации

**1. Цели защиты и виды угроз**

**Защита информации** - это комплекс мероприятий, направленных на обеспечение важней­ших аспектов информационной безопасности, а именно целостности, доступности и, если нужно, конфиденциальности информации и ресурсов. **Система называется безопасной,** если она, исполь­зуя соответствующие аппаратные и программные средства, управляет доступом к информации так, что только должным образом авторизированные лица имеют право получать, создавать или изме­нять информацию. **Цель защиты** - предупреждение несанкционированной модификации информа­ции.

Нарушение целостности, достоверности и конфиденциальности информации может произой­ти как случайно, т.е. без злого умысла, так и преднамеренно для принесения ущерба владельцу ин­формации или извлечения выгоды.

Под **угрозой** информации понимают меру возможности возникновения такого явления или события, следствием которого могут быть нежелательные воздействия на информацию: нарушение физической целостности, несанкционированное получение, модификация или размножение инфор­мации.

Классификация **по цели реализации угрозы:**

* Нарушение конфиденциальности информации, т.е. несанкционированное использование, на­носящее ущерб владельцу информации;
* Нарушение целостности информации, удаление или внедрение дезинформации;
* Частичное или полное нарушение работоспособности информационной системы.

Классификация по **субъекту реализации угрозы:**

* Угрозы, реализация которых выполняется при постоянном участии человека;
* Угрозы, реализация которых выполняется с помощью специальных компьютерных программ без участия человека.

**Задачи по защите** от всех видов угроз одинаковы:

* Преградить несанкционированный доступ к ресурсам вычислительных систем;
* Сделать невозможным несанкционированное использование компьютерных ресурсов, даже если доступ осуществлен;
* Своевременно обнаружить факт несанкционированных действий и устранить причины и по­следствия их реализации.

Таким образом, необходимо создание комплексной системы защиты информационных систем как от случайных факторов, нарушающих целостность информации, так и от преднамеренных не­санкционированных действий.



**2. Методы защиты информации**

1. Методы защиты от **сбоев оборудования:**
	* + **периодическое архивирование** программ и данных. Под архивированием понимается как соз­дание простой резервной копии, так и создание копии с предварительным сжатием (компресси­ей) информации. В последнем случае используются специальные программы-архиваторы (Arj, Rar, Zip и др.);
		+ **автоматическое резервирование** файлов. При использовании программ автоматического ре­зервирования команда на сохранение любого файла автоматически дублируется и файл сохра­няется на двух автономных носителях (например, на двух винчестерах). Выход из строя одного из них не приводит к потере информации. Резервирование файлов широко используется, в ча­стности, в банковском деле.
2. Методы защиты от **случайной потери** или **искажения информации,** хранящейся в компью­тере:
* **автоматический запрос на подтверждение команды,** приводящей к изменению содержимого какого-либо файла. Если нужно удалить файл **или** разместить новый файл под именем уже существующего, на экране дисплея появляется диалоговое окно с требованием подтверждения команды либо её отмены;
* **установка специальных атрибутов документов.** Например, многие программы-редакторы по­зволяют сделать документ доступным только для чтения или скрыть файл, сделав недоступным его имя в программах работы с файлами;
* **возможность отменить последние действия.** При редактуре документа, можно пользоваться функцией отмены последнего действия или группы действий. Если ошибочно удален нужный файл, то специальные программы позволяют его восстановить (правда, только в том случае, ко­гда ничего не записано поверх удаленного файла);
* **разграничение доступа пользователей** к ресурсам файловой системы, строгое разделение системного и пользовательского режимов работы вычислительной системы.
1. **Методы защиты информации от несанкционированного (нелегального) доступа:**
* **криптографическое шифрование информации.** Заключается в таком преобразовании защи­щаемой информации, при котором по внешнему виду нельзя определить содержание закрытых данных, а прочтение или восстановление информации возможно только при знании ключа. **Ключ** - это информация, необходимая для беспрепятственного шифрования и дешифрования текста. Криптографическая защита считается наиболее надежной, а для информации, переда­ваемой по линии связи большой протяженности - единственным средством защиты информации от хищений.
* **применение** паролей, которые позволяют контролировать доступ как к компьютерам, так и к отдельным программам или файлам. Эффективность парольных методов значительно повыша­ется при использовании нетривиальных или длинных зашифрованных паролей, записанных на информационные носители. Существуют также программные средства защиты от «вскрытия» паролей - операционные системы могут отслеживать случаи, когда многократно употребляются неверные пароли и блокировать доступ к системе. Более сложная защита (называемая ловуш­кой) — это ложный доступ к информации на время, пока идет поиск местонахождения взломщи­ка.
* **программно-аппаратные средства защиты** от незаконного копирования программ и данных, в частности находящихся на коммерчески распространяемых носителях информации. Например «электронные замки», позволяющие сделать с диска не более установленного числа копий, или дающие возможность работать с программой только при условии, что к специальному разъёму системного блока подключено устройство (обычно микросхема), поставляемое вместе с легаль­ными копиями программ.
1. Защита информации от **компьютерных вирусов**

**Вирус** представляет собой самовоспроизводящуюся программу, которая способна внедрять свои копии в файлы, системные области, вычислительные сети и т. д. и приводить к нарушению нормального функционирования компьютера. Копии вирусной программы также сохраняют способ­ность дальнейшего распространения.

**Основные источники вирусов:**

* флешка, на которой находятся зараженные вирусом файлы;
* компьютерная сеть, в том числе электронная почта и Internet;
* жесткий диск, на который попал вирус в результате работы с зараженными программами
* вирус, оставшийся в оперативной памяти после предшествующего пользователя.

**Основные ранние признаки заражения компьютера вирусом:**

* уменьшение объема свободной оперативной памяти; замедление загрузки и работы компьютера;
* непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней
* модификации файлов;
* ошибки при загрузке операционной системы;
* невозможность сохранять файлы в нужных каталогах;
* непонятные системные сообщения, музыкальные и визуальные эффекты и т.д.

**Признаки активной фазы вируса:**

* исчезновение файлов;
* форматирование жесткого диска;
* невозможность загрузки файлов или операционной системы.

По **деструктивным возможностям** вирусы разделяют на:

* **безвредные** вирусы проявляются только в том, что уменьшают объем памяти на диске в ре­зультате своего распространения.
* **неопасные** вирусы также уменьшают объем памяти и кроме того порождают графические, зву­ковые и другие эффекты.
* **опасные** вирусы могут привести к нарушениям нормальной работы компьютера, например к за­висанию или к неправильной печати документа.
* **очень опасные вирусы** могут привести к уничтожению программ и данных, стиранию инфор­мации в системных областях памяти и даже приводить к выходу из строя движущихся частей жесткого диска при вводе в резонанс.

**По среде обитания** вирусы разделяют на **файловые, загрузочные и сетевые:**

* **файловые** вирусы внедряются в выполняемые файлы (с расширением .exe, .com), или файлы текстовых редакторов и табличных процессоров.
* **загрузочные** вирусы внедряются в загрузочный сектор диска или в сектор системного загрузчи­ка жесткого диска.
* **сетевые** вирусы распространяются по компьютерной сети.

По **особенностям алгоритмов** различают следующие вирусы:

* 1. **вирусы-невидимки или STEALTH-вирусы** искажают информацию, прочитанную с диска так, что программа, которой предназначена эта информация, получает неверные данные;
	2. **ретро-вирусы** заражают антивирусные программы, стараясь уничтожить их или сделать нетру­доспособными;
	3. **вирусы-черви** снабжают небольшие сообщения электронной почты, так называемым заголов­ком, который по своей сути есть Web-адрес местонахождения самого вируса. При попытке про­читать такое сообщение вирус начинает считывать через глобальную сеть internet свое 'тело' и после загрузки начинает деструктивное действие. Очень опасные, так как обнаружить их очень тяжело; »
	4. **паразитические вирусы** при распространении меняют содержимое дисковых секторов и фай­лов и, как следствие, легко обнаруживаются;
	5. **вирусы-призраки** представляют собой трудно обнаруживаемые вирусы, которые имеют за­шифрованное тело вируса, благодаря чему две копии одного вируса не имеют одинаковых уча­стков кода (сигнатур).

**К общим средствам, помогающим предотвратить заражение относят**:

* резервное копирование информации (создание копий файлов и системных областей жестких дисков);
* отказ от использования случайных и неизвестных программ (т.к. чаще всего вирусы распростра­няются вместе с компьютерными программами);
* перезагрузка компьютера перед началом работы, особенно, если за этим компьютером работа­ли другие пользователи;
* ограничение доступа к информации, в частности физическая защита носителя информации во время копирования файлов с нее.
* специализированные антивирусные программы.

***Антивирус*** - это программа, выявляющая и обезвреживающая компьютерные вирусы.

Антивирусные программы относятся к программным средствам защиты.

*(Следует заметить, что вирусы в своем развитии опережают антивирусные программы, поэтому даже в случае регулярного пользования антивирусов, нет 100% гарантии безопасности. Антивирусные программы могут выявлять и уничтожать лишь известные вирусы, при появле­нии нового компьютерного вируса защиты от него не существует до тех пор, пока для него не будет разработан свой антивирус. Однако, много современных антивирусных пакетов имеют в своем составе специальный программный модуль, называемый эвристическим анализатором, который способен исследовать содержимое файлов на наличие кода, характерного для компью­терных вирусов. Это дает возможность своевременно выявлять и предупреждать об опасности заражения новым вирусом.)*

Различают следующие типы антивирусных программ:

* + 1. ***программы-детекторы*:** предназначены для нахождения зараженных файлов одним из извест­ных вирусов, они могут также лечить файлы от вирусов или уничтожать зараженные файлы.
		2. ***программы-лекари*:** предназначены для лечения зараженных дисков и программ. Лечение про­граммы состоит в изъятии из зараженной программы тела вируса.
		3. ***программы-ревизоры*:** предназначены для выявления заражения вирусом файлов, а также на­хождение поврежденных файлов. Эти программы запоминают данные о состоянии программы и системных областей дисков в нормальном состоянии (до заражения) и сравнивают эти данные в процессе работы компьютера, в случае несоответствия данных выводится сообщение о возмож­ности заражения;
		4. ***лекари-ревизоры***: предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние.
		5. ***программы-фильтры***: предназначены для перехвата обращений к операционной системе, которые используются вирусами для размножения и сообщают об этом пользователю, который может разрешить или запретить выполнение соответствующей операции.
		6. ***программы-вакцины*:** используются для обработки файлов и загрузочных секторов с целью предупреждения заражения известными вирусами. Суть вакцинации заключается в модифика­ции программ или диска таким образом, чтобы это не отражалось на нормальном выполнении программ и то же время вирусы воспринимали их как уже зараженные и поэтому не пытались внедриться, (в последнее время этот метод используется все чаще).

Для достижения максимального эффекта защиты от вирусов рекомендуется использовать не­сколько разных антивирусных пакетов одновременно.

2.5. **Административные и правоохранительные методы защиты информации:**

Разрешение различных конфликтов в области информационных отношений на базе дейст­вующего законодательства возможно только для документированной информации (ст. 4.1, ст.6.1).

Информационные ресурсы, т.е. отдельные документы или массивы документов, в том числе и в ин­формационных системах, являясь объектами отношений физических, юридических лиц и государст­ва, подлежат обязательному учёту и защите как материального имущества собственника.

Собствен­нику предоставляется право самостоятельно в пределах своей компетенции устанавливать режим защиты информационных ресурсов и доступа к ним (ст.6.7).

**Закон "Об информации"** гласит: **-документированная информация** *ограниченного доступа по условиям её правового режима под­разделяется на информацию, отнесённую к государственной тайне и конфиденциальную* (ст.Ю, ч.2); **-конфиденциальная информация** - *документированная информация, доступ к которой ограничи­вается в соответствии с законодательством РФ* (ст.2);

* **персональные** *данные, включаемые в состав федеральных информационных ресурсов, совмест­ного ведения, федерального и местного самоуправления, а также получаемые и собираемые него­сударственными организациями, отнесены к категории конфиденциальной информации* (ст.11, ч.1);
* **не допускается сбор, хранение, использование** и **распространение информации о частной** жизни, *а равно информации, нарушающей личную тайну, тайну переписки, телефонных переговоров и т.д. физического лица без его согласия, кроме как на основании судебного решения* (ст. 11, ч.1).

**Ответственность за преступления в области информационных технологий**

Составы компьютерных преступлений (перечень признаков, характеризующих общественно опасное деяние как конкретное преступление) приведены в главе 28 Уголовного Кодекса РФ (введён в действие 1.1.1997 г.), которая называется *"Преступление в сфере компьютерной информа­ции"* и содержит *3 статьи:*

1. **"Неправомерный доступ к компьютерной информации" (ст. 272);**

**Статья** 272 предусматривает ответственность за несанкционированный доступ, если это по­влекло уничтожение, блокировку, модификацию или копирование информации, нарушение работы вычислительных систем. Обычно несанкционированный доступ осуществляется умышленно (лише­ние свободы до 2-х лет, и до 5-ти лет , если преступление совершено группой лиц).

* 1. **"Создание, использование и распространение вредоносных программ для ЭВМ (ст.** **273).**

**Статья** 273. Преступление, предусмотренное ч.1 ст. 273, может быть совершено умышленно и максимальным наказанием является лишение свободы до 3-х лет.

* 1. **'Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети" (ст. 274).**

**Статья 274.** Обычно нарушение Правил эксплуатации осуществляется умышленно. Преступ­ление наказывается лишением права занимать определённые должности или заниматься опреде­лённой деятельностью на срок до 5-ти лет.

**Литература**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
4. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
5. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)

**Лекция № 15**

**Криптографическое закрытие**

* 1. Классификация методов криптографического закрытия
	2. Методы криптографического закрытия
	3. Криптографические системы
	4. Криптографические стандарты

Криптографические методы защиты основаны на возможно­сти осуществления некоторой операции преобразования инфор­мации, которая может выполняться одним или несколькими пользователями СОИ, обладающими некоторым секретом, без знания которого (с вероятностью, близкой к единице, за разум­ное время) невозможно осуществить эту операцию.

* 1. **Классификация методов криптографического закрытия**

Рассмотрим классификацию методов криптографического закрытия.

Под***шифрованием*** понимается такой вид криптографическо­го закрытия, **при котором преобразованию подвергается каждый символ защищаемого сообщения**.

Все известные способы шиф­рования можно разбить на пять групп: подстановка (замена), перестановка, аналитическое преобразование, гаммирование и комбинированное шифрование. Каждый из этих способов мо­жет иметь несколько разновидностей.

Под***кодированием*** понимается такой вид криптографическо­го закрытия, **когда некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее вы­бранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями и т. п.)**. Этот метод имеет две разновидности: смысловое и символьное кодирование. При смысловом кодиро­вании кодируемые элементы имеют вполне определенный смысл (слова, предложения, группы предложений). При символьном кодировании кодируется каждый символ защищаемого сообще­ния. Символьное кодирование по существу совпадает с шифро­ванием заменой.

***Перестановки*** *—* несложный метод криптографического пре­образования. Используется как правило в сочетании с другими методами.

**Методы криптографического закрытия**

|  |
| --- |
| ***Шифрование – вид криптографическо­го закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения*** |
| **Замена (подстановка)** – символы шифруемого текста заменяются другими символами, взятыми из *одного*  или *нескольких*  алфавитов | Простая (одноалфавитная) |
| Многоалфавитная одноконтурная обыкновенная |
| Многоалфавитная одноконтурная монофоническая |
| Многоалфавитная многоконтурная |
| **Перестановка** – символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. | Простая |
| Усложненная по таблице |
| Усложненная по маршрутам |
| **Аналитическое преобразование** | С использованием алгебры матриц |
| По особым зависимостям |
| **Гаммирование** – наложении на ис­ходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа | С конечной короткой гаммой |
| С конечной длинной гаммой |
| С бесконечной гаммой |
| **Комбинированные методы** | Замена и перестановка |
| Замена и гаммирование |
| Перестановка и гаммирование |
| Гаммирование и гаммирование |
| ***Кодирование –*** ***вид криптографическо­го закрытия, когда некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее вы­бранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями и т. п.).*** |
| **Смысловое** | По специальным таблицам (словарям) |
| **Символьное** | По кодовому алфавиту |
| **Другие *виды*** |
| **Рассечение-разнесение** – массив защищаемых данных де­лится (рассекается) на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации | Смысловое |
| Механическое |
| **Сжатие-расширение** – замена часто встречаю­щихся одинаковых строк данных или последовательностей оди­наковых символов некоторыми заранее выбранными символами |  |

*Многоалфавитная подстановка* – наиболее простой вид пре­образований, заключающийся в замене символов исходного тек­ста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

*Гаммирование —* этот метод заключается в наложении на ис­ходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

***Блочные шифры*** представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого тек­ста. Блочные шифры на практике встречаются чаще, чем «чис­тые» преобразования того или иного класса в силу их более вы­сокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе шифров.

*Комбинированные методы шифрования.* Вообще говоря, ком­бинировать можно любые методы шифрования и в любом коли­честве, однако на практике наибольшее распространение полу­чили следующие комбинации: 1) подстановка + гаммирование; 2) перестановка + гаммирование; 3) гаммирование + гаммирова­ние; 4) подстановка + перестановка. Типичным примером ком­бинированного шифра является национальный стандарт США криптографического закрытия данных (DES).

К отдельным видам криптографического закрытия относятся методы *рассечения-разнесения и сжатия данных.* Рассечение-раз­несение заключается в том, что массив защищаемых данных де­лится (рассекается) на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Выделенные таким образом элементы данных раз­носятся по разным зонам ЗУ или располагаются на различных носителях. Обратная процедура называется сборкой данных. Совершенно очевидно, что алгоритм разнесения и сборки дан­ных должен тщательно охраняться.

Сжатие данных представляет собой замену часто встречаю­щихся одинаковых строк данных или последовательностей оди­наковых символов некоторыми заранее выбранными символами.

Кратко рассмотрим основные методы криптографического закрытия информации.

***Шифрование заменой (подстановка).*** В этом, наиболее про­стом, методе символы шифруемого текста заменяются другими символами, взятыми из *одного (одно- или моноалфавитная под­становка)* или *нескольких (много- или полиалфавитная подстанов­ка)* алфавитов.

Самой простой разновидностью является *прямая (простая) замена,* когда буквы шифруемого сообщения заменяются други­ми буквами того же самого или некоторого другого алфавита. Таблица замены может иметь следующий вид.

**Таблица простой замены**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Исходные символы шифруемого текста | А | В | C | D | Е | F | *G* | Н | I | J | К | L | М | N | 0 | Р | Q | R | S | Т | U | V | W | X | Y | Z |
| Заменяемые символы | S | P | X | L | R | Z | I | М | А | Y | Е | D | W | Т | В | G | V | N | J | О | C | F | Н | Q | U | К |

Используя эту таблицу, зашифруем текст:

***In this book the reader will find a comprehensive survey...***

Получим следующее зашифрованное сообщение:

***At omiy pbbe omr nrsirn fadd zail s xbwgnrmrtjafr jcnfru. . .***

Однако такой шифр имеет низкую стойкость, так как за­шифрованный текст имеет те же статистические характеристики, что и исходный. Например, текст на английском языке содержит символы со следующими частотами появления (в порядке убы­вания): ***Е—*** 0,13, ***Т*** — 0,105; ***А*** - 0,081, ***О*** - 0,079 и т. д. В за­шифрованном тексте наибольшие частоты появления в порядке убывания имеют буквы ***R*** — 0,12; ***О —*** 0,09, ***А*** и ***N*** по 0,07.

Естественно предположить, что символом ***R*** зашифрована буква ***Е,*** символом ***О*** — букв ***Т*** и т. д. Это действительно соот­ветствует таблице замены. Дальнейшая расшифровка не состав­ляет труда. Эти методы дешифровки хорошо известны из клас­сической литературы (см., например, Артур Конан Дойль «Пля­шущие человечки», или Алан Эдгар По «Золотой жук»).

Если бы объем зашифрованного текста был намного больше, чем в рассмотренном примере, то частоты появления букв в за­шифрованном тексте были бы еще ближе к частотам появления букв в английском алфавите и расшифровка была бы еще про­ще. Поэтому простую замену используют редко и лишь в тех случаях, когда шифруемый текст короток.

Для повышения стойкости шифра используют***полиалфавит­ные подстановки***, в которых для замены символов исходного тек­ста используются символы нескольких алфавитов.

Частным случаем рассмотренной***полиалфавитной замены*** яв­ляется так называемая***монофоническая замена****.* Особенность это­го метода состоит в том, что количество и состав алфавитов вы­бираются таким образом, чтобы частоты появления всех симво­лов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статистической обработки. *Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается использование большего числа заменяющих элементов, чем для редко встречающихся*. Пример монофонического шифра для английского алфавита показан в таблице. Шифрование осуще­ствляется так же, как и при простой замене (т. е. по шифрующе­му алфавиту № 1) с той лишь разницей, что после шифрования каждого знака соответствующий ему столбец алфавитов цикли­чески сдвигается вверх на одну позицию. Таким образом, столб­цы алфавита как бы образуют независимые друг от друга кольца, поворачиваемые вверх на один знак каждый раз после шифрова­ния соответствующего знака. В качества примера зашифруем монофоническим шифром тот же текст, который шифровался простой заменой:

*In this book the reader will find a comprehensive survey.. .*

Шифрованный текст имеет вид:

*А(-,) VNG/LjpGZ+F.=hg...*

Если подсчитать частоты появления символов, то легко ви­деть, что даже на таком коротком образце текста они в значи­тельной мере выровнены.

***Шифрование методом перестановки*** заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов.

**Монофонический шифр для английского алфавита**

|  |
| --- |
| Алфавит открытого текста |
| А | В | С | D | Е | F | G | H | I | j | К | L | M | N | 0 | р | Q | R | S | т | и | V | w | X | Y | Z |
| f | N | Q |  | G | T | D | , | A | e | L | - | R | ( | С | X | I | Z | V | — | w | s | h | u | К | t |
| \* | N | Q | Ь | + | t | D | P | ) | e | L | 0 | R | У | / | X | I | = | $ | j | w | s | h | u | К | t |
| к | N | 0 | i | 1 | W | D | r | q | e | L | и | R | ( | # | X | I | а | d |  | w | s | h | u | К | t |
| £ | N | Q |  | 1 | T | D | , | A | e | L | A. | R | Y | n | X | I | Z | V | с | w | s | h | u | К | t |
| \* | N | Q | Ь | G | [ | D | P | ) | e | L | 0 | R | ( | С | X | I | = | 5 | -- | w | s | h | u | К | t |
| R | Ы | 0 | i | + | w | D | r | q | e | L | И | R | Y | / | X | I | а | d | i | w | s | h | u | К | t |
| f | N | Q |  | ] | T | D |  | A | e | L | A. | R | ( | # | X | I | 2 | V |  | и | s | h | u | К | t |
| \* | N | Q | b | 1 | [ | D | p | ) | e | L | 0 | R | Y | п | X | I | = | $ | с | w | s | h | u | К | t |
| к | N | Q | i | G | w | D | r | q | e | L | и | R | ( | с | X | I | а | d | — | w | s | h | u | К | t |
| f | N | 0 |  | + | T | D |  | A | e | L | 0 | R | Y | */* | X | I | *Z* | V | i | w | s | h | u | К | t |
| \* | N | Q | Ь | ] | [ | D | p | ) | e | L | A | R | ( | # | X | I | = | $ |  | w | s | h | u | К | t |
| к | N | Q | i | 1 | w | D | r | q | e | L | и | R | Y | п | X | I | а | d | с | w | s | h | u | К | t |

Рассмотрим не­которые наиболее часто встречающиеся разновидности этого ме­тода, которые могут быть использованы в автоматизированных системах.

Самая простая перестановка — написать исходный текст за­дом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ, получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП.

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его допол­нить незначащей буквой (например, О) до числа, кратного пяти:

ПУС ТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительное из­менение, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется, ничего сложного, но при расшифровке проявятся серьезные неудобства.

Текст может быть размещен в прямоугольной решетке однако для обмена информацией требуются предварительные договоренности между адресатом и отправителем по­сланий, поскольку сама решетка может быть различной длины-высоты, записывать в нее можно по строкам, по столбцам, по спирали, по диагоналям, а для шифрования можно брать тоже различные направления.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| П | У | С | Т | Ь | Б |
|  У | Д | Е | Т | Т | А |
| К | К | А | К | М | Ы |
| Х | О | Т | Е | Л | И |
| А | Б | В | Г | Д | Е |
| М | Л | К | И | З | Ж |

 Перестановка с прямой решеткой |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Решетка Кардано |

|  |  |  |  |
| --- | --- | --- | --- |
| И | Р | М | Т |
| Г | О | У | С |
| Й | О | У | Г |
| Р | Е | Р | Д |

 |

Для примера возьмем решетку 6x6 (причем количество строк может увеличиваться или уменьшаться в зависимости от длины исходного сообщения) и заполним ее по строкам. Если шифровать по диагоналям (стрелкам) сверху вниз с левого верх­него угла, то в итоге получится такая шифрограмма:

П УУ СДК ТЕКХ ЬТАОА БТКТБП АМЕВР ЫЛГС ИДТ ЕУ Ф

Для окончательного оформление шифротекст может быть разбит на группы по 6 символов

ПУУСДК ТЕКХЬТ АОАБТП ТБМАМЕ ВРЬШГС ИДТЕУФ

Интересным примером является ***решетка Кардано*** *– метод перестановки, базирующийся на решетчатой маске, устроенной таким образом, что при каждом повороте на 90° отверстия открывают участки чистой бумаги, а за 4 поворота «лист» (в данном случае 4x4) заполняется полностью.* Самостоятельно расшифруйте фрагмент текста на рисунке (МОЙ ДРУГ РИСУЕТ РОГ)*.*

Из рассмотренных примеров очевидно, что все процедуры шифрования и расшифровки по методу перестановок являются в достаточной степени формальными и могут быть реализованы алгоритмически.

***Шифрование методом гаммирования*** **состоит в том, что сим­волы шифруемого текста последовательно суммируются с сим­волами некоторой служебной последовательности, которая на­зывается гаммой.** Иногда такой метод представляют как наложе­ние гаммы на исходный текст, поэтому он получил название «гаммирование».

Пример гаммирования приведен на рисунке – символы ис­ходного текста и гаммы представляются в виде двоичного кода,

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Символы шифруемого текста | Б | У | Д | Ь | …  |
| 010010 | 100000 | 110010 | 100000 | … |
| Знаки гаммы: десятичные  двоичные | 7000111 | 1000001 | 8001000 | 2000010 | … |
| Символы зашифрованного текста | 010101 | 100001 | 111010 | 100010 | … |

**Пример шифрования гаммированием**

затем соответствующие разряды складываются по модулю 2. Вместо сложения по модулю 2 при гаммировании можно ис­пользовать и другие логические операции.

Стойкость шифрования методом гаммирования определяется главным образом свойствами гаммы — длительностью периода и равномерностью статистических характеристик. Последнее свой­ство обеспечивает отсутствие закономерностей в появлении раз­личных символов в пределах периода.

*Обычно разделяют две разновидности гаммирования — с ко­нечной и бесконечной гаммами*. При хороших статистических свойствах гаммы стойкость шифрования определяется только длиной периода гаммы. *При этом, если длина периода гаммы превышает длину шифруемого текста, то такой шифр теоретиче­ски является абсолютно стойким, т. е. его нельзя вскрыть с по­мощью статистической обработки зашифрованного текста.* Это, однако, не означает, что дешифрование такого текста вообще невозможно: при наличии некоторой дополнительной информа­ции исходный текст может быть частично или полностью вос­становлен даже при использовании бесконечной гаммы.

В качестве гаммы может быть использована любая последо­вательность случайных символов, например, последовательность цифр числа π, числа *е* (основание натурального логарифма) и т. п. При шифровании с помощью ЭВМ последовательность гаммы может формироваться с помощью датчика псевдослучай­ных чисел (ПСЧ) – известно несколько алгоритмов работы та­ких датчиков, которые обеспечивают удовлетворительные харак­теристики гаммы.

Обычно для генерации последовательности псевдослучайных чисел применяют компьютерные программы, которые, хотя и называются генераторами случайных чисел, на самом деле выдают детерминированные числовые последовательности, которые по своим свойствам очень похожи на случайные.

*К криптографически стойкому генератору псевдослучайной последовательности чисел (гаммы шифра) предъявляются три основных требования*:

• период гаммы должен быть достаточно большим для шифрования сообщений различной длины;

• гамма должна быть практически непредсказуемой, что означает невозможность предсказать следующий бит гаммы, даже если известны тип генератора и предшествующий кусок гаммы;

• генерирование гаммы не должно вызывать больших технических сложностей.

Длина периода гаммы является самой важной характеристикой генератора псевдослучайных чисел. По окончании периода числа начнут повторяться, и их можно будет предсказать. Требуемая длина периода гаммы определяется степенью закрытости данных. Чем длиннее ключ, тем труднее его подобрать. Длина периода гаммы зависит от выбранного алгоритма получения псевдослучайных чисел.

***Шифрование с помощью аналитических преобразований.*** Доста­точно надежное закрытие информации может быть обеспечено при использовании для шифрования некоторых аналитических преобразований. Для этого можно использовать методы алгебры матриц, например, умножение матрицы на вектор по правилу:

С = А х В; сi =$\sum\_{j=1}^{N}a\_{ij}b\_{j}$

Если матрицу А = ***(atj)*** использовать в качестве ключа, а вме­сто компонента вектора В = ***bj*** подставить символы текста, то компоненты вектора С = (сi) будут представлять собой символы зашифрованного текста.

Приведем пример, взяв в качестве ключа квадратную матри­цу третьего порядка

***A*** = $\left(\begin{matrix}14&8&3\\8&5&2\\3&2&1\end{matrix}\right)$

Заменим буквы алфавита цифрами, соответствующими их порядковому номеру в алфавите: А – О, Б – 1, В – 2, и т. д. Тогда отрывку текста **ВАТАЛА** будет соответствовать последовательность 2, 0, 19, 0, 12, 0. По принятому алгоритму шифрования выполним необходимые действия с тройками символов: С = А х В

При этом зашифрованный текст примет вид: 85, 54, 25, 96, 60, 24.

Дешифрование осуществляется с использованием того же правила умножения матрицы на вектор, только в качестве ключа берется матрица, обратная той, с помощью которой осуществляется зашифровка, а в качестве вектора-сомножителя соответ­ствующие фрагменты символов закрытого текста; тогда значениями вектора-результата будут цифровые эквиваленты знаков открытого текста.

$$А^{-1}=\left(\begin{matrix}1&-2&1\\-2&5&-4\\1&-4&6\end{matrix}\right)$$

Таким образом, получена последовательность знаков раскрытого текста 2, 0, 19, 0, 12, 0, что соответствует исходному тексту. *Этот метод шифрования является формальным, что позволяет легко реализовать его программными средствами*.

***Кодирование.*** Одним из средств криптографического закрытия информации, также имеющим длительную историю практического использования, является кодирование, **под которым понимается замена элементов закрываемых данных некоторыми цифровыми, буквенными или комбинированными сочетаниями – кодами**. Нетрудно заметить, что между кодированием информации и ее шифрованием подстановкой существует значительная аналогия. Однако между этими методами можно найти и различия.

При шифровании подстановкой заменяемыми единицами информации являются символы алфавита, и, следовательно, шифрованию могут подвергаться любые данные, для фиксирования которых используется данный алфавит. При кодировании замене подвергаются смысловые элементы информации, поэтому для каждого специального сообщения в общем случае необходимо использовать свою систему кодирования. Правда, в последнее время разработаны специальные коды, имеющие целью сократить объем информации при записи ее в ЗУ. Специфика этих кодов заключается в том, что для записи часто встречающихся символов используются короткие двоичные коды, а для записи редко встречающихся – длинные.

Примером такого кода для английского языка может служить код Хаффмана, показанный в таблице.

**Коды Хаффмана**

|  |  |
| --- | --- |
| Символы | Кодовые последовательности |
| **А** | 1 | 1 | 1 | 1 |  |  |  |  |  |  |
| **O** | 1 | 1 | 1 | 0 |  |  |  |  |  |  |
| **N** | 1 | 1 | 0 |  |  |  |  |  |  |  |
| **D** | 1 | 1 | 0 | 1 | 1 |  |  |  |  |  |
| **Р** | 1 | 1 | 0 | 1 | 0 | 1 |  |  |  |  |
| **V** | 1 | 1 | 0 | 1 | 0 | 0 | 1 |  |  |  |
| **К** | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |  |
| **Q** | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| **Z** | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| **X** | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |  |
| **J** | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |  |
| **R** | 1 | 0 | 1 | 1 |  |  |  |  |  |  |
| **I** | 1 | 0 | 1 | 0 |  |  |  |  |  |  |
| **Е** | 1 | 0 | 0 |  |  |  |  |  |  |  |
| **S** | 0 | 1 | 1 | 0 |  |  |  |  |  |  |
| **W** | 0 | 1 | 1 | 1 | 0 | 1 |  |  |  |  |
| **B** | 0 | 1 | 1 | 1 | 0 | 0 |  |  |  |  |
| **H** | 0 | 1 | 0 | 1 |  |  |  |  |  |  |
| **F** | 0 | 1 | 0 | 0 | 1 |  |  |  |  |  |
| **С** | 0 | 1 | 0 | 0 | 0 |  |  |  |  |  |
| **M** | 0 | 0 | 0 | 1 | 1 |  |  |  |  |  |
| **U** | 0 | 0 | 0 | 1 | 0 |  |  |  |  |  |
| **G** | 0 | 0 | 0 | 0 | 1 |  |  |  |  |  |
| **Y** | 0 | 0 | 0 | 0 | 0 |  |  |  |  |  |

Такое кодирование имеет криптографическую стойкость на уровне шифрования простой заменой.

При смысловом кодировании основной кодируемой единицей является смысловой элемент текста. Для кодирования составляется специальная таблица кодов, содержащая перечень кодируемых элементов и соответствующих им кодов. Введем, на­пример, следующую кодовую таблицу:

Автоматизированные системы управления 001

Автоматизация управления 002

Осуществляет 415

Позволяет 632

Тогда предложение Автоматизированные системы управления позволяют осуществлять автоматизацию управления . . . после кодирования будет иметь вид: 001632 415 002....

**3.Криптографические системы**

Рассмотренные понятия в настоящее время объединяются в укрупненную концепцию криптографических систем (криптосистем).

Сущность процессов в криптосистемах заключается в сле­дующем. Сообщение (текст, аудио- или видеоизображение) пре­образуется (шифруется) с помощью известного математического алгоритма и некоторого «ключа» так, что восстановление (де­шифрирование) и прочтение первоначального текста (восста­новление аудио- или видеоизображения) становятся возможны­ми, если известны алгоритм и «ключ». Последний же обязатель­но должен быть известен только источнику и получателю сообщения.

Используются, как правило, два типа криптосистем:

* симметричные (одноключевые) системы, основанные на использовании закрытых, секретных ключей;
* асимметричные системы, в которых используются один от­крытый и один закрытый ключ. Эти алгоритмы называют­ся также асимметричными.

***Одноключевая (классическая) криптография*** использует только одну единицу секретной информации — ключ, знание которого позволяет отправителю зашифровать информацию, а получате­лю — расшифровать ее (рис.1). Именно эти операции шифро­вания/расшифрования с большой вероятностью невыполнимы без знания секретного ключа. Поскольку обе стороны, владею­щие ключом, могут как шифровать, так и расшифровывать ин­формацию, такие алгоритмы преобразования называют симмет­ричными или алгоритмами с секретным (закрытым) ключом.

декретный» ключ



**Рис.1 Симметричная криптосистема**

При ее использовании возникает сложная задача обеспече­ния надежного закрытого канала для обмена ключами.

***Асимметричная система.*** В криптографии с открытым клю­чом имеется два ключа, по крайней мере один из которых нель­зя вычислить из другого. Один ключ используется отправителем для шифрования информации, закрытие которой необходимо обеспечить. Другой ключ используется получателем для расшиф­ровки полученной информации. Бывают приложения, в которых один ключ должен быть несекретным, а другой — секретным. Алгоритмы преобразования с открытым и секретным ключами называют асимметричными, поскольку роли сторон, владеющих разными ключами из пары, различны (рис. 2).

Адресат-источник А, посылая адресату-получателю Б сооб­щение, шифрует его, используя известный открытый ключ або­нента Б. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сооб­щения возможно только с использованием закрытого ключа, который известен только адресату Б. Адресат Б, получив от адре­сата А сообщение, расшифровывает его с помощью своего за­крытого ключа.

Открытый ключ Закрытый ключ

абонента Б абонента Б



**Рис. Асимметричная криптосистема**

Таким образом в организованной информационной конфи­денциальной сети каждый абонент должен знать и хранить втай­не свой уникальный закрытый ключ и список открытых ключей тех абонентов, с которыми он должен поддерживать информаци­онную связь.

*Применение криптографических методов и средств*

Криптографические системы, реализованные в виде про­грамм, встраиваются в программное обеспечение существующих рабочих станций и серверов и тем самым позволяют организо­вать защиту конфиденциальной информации как при ее хране­нии (в зашифрованном виде) и обработке в информационных системах, так и при передаче по каналам связи телекоммуника­ционных сетей.

С помощью рассмотренных криптографических методов ре­шаются такие основные задачи, как:

* предотвращение возможности несанкционированного оз­накомления с информацией при ее хранении в компьютере или на отчуждаемых носителях, а также при передаче по каналам связи;
* обнаружение искажений или ошибок, возникающих при передаче информации по каналам связи телекоммуникаци­онных сетей;
* подтверждение подлинности электронного документа, до­казательство авторства документа и факта его получения от соответствующего источника информации;

***Защита от доступа.*** Первая задача решается шифрованием информации (данных). Зашифрованное сообщение становится недоступным для лиц, не допущенных к соответствующей ин­формации, т. е. не знающих ключа, с помощью которого можно расшифровать сообщение. Перехват зашифрованных данных в этом случае бесполезен.

***Защита от искажений.*** Для защиты данных от случайных или преднамеренных искажений в канале связи используется контрольная последовательность — имитовставка. Она выраба­тывается путем криптографического преобразования шифруемо­го сообщения и ключа шифрования и представляет собой после­довательность данных фиксированной длины. Имитовставка пе­редается по каналу связи вместе с зашифрованным сообщением. Поступившее зашифрованное сообщение расшифровывается, вырабатывается контрольная имитовставка, которая сравнивает­ся с имитовставкой, полученной из канала связи. В случае не­совпадения имитовставок все расшифрованные данные считают­ся искаженными и бракуются.

***Электронная цифровая подпись.*** Проблема установления ис­тинности документа и личности подписавшего этот документ лица приобретает особое значение во многих системах, связан­ных с юридической ответственностью за принимаемые решения, таких, как системы государственного и военного управления, финансовые и банковские системы, системы, связанные с рас­пределением материальных ценностей, и другие. Эта проблема решается с помощью так называемой электронной подписи (ЭЦП), которая дает возможность заменить традиционные пе­чать и подпись и, не меняя самого документа, позволяет прове­рить подлинность и авторство полученной информации. Для вы­работки электронной подписи также используются методы асим­метричных криптографических преобразований.

Каждый пользователь, обладающий правом подписи, само­стоятельно формирует личные закрытый и открытый ключи подписи. Закрытый ключ подписи используется для выработки электронной цифровой подписи и должен сохраняться пользова­телем втайне, что гарантирует невозможность подделки доку­мента и цифровой подписи от его имени злоумышленником.

Открытый ключ используется для проверки подлинности до­кумента, а также для предупреждения отказа подписавшего его от своей подписи. Знание открытого ключа не дает возможности определить секретный ключ. Открытые ключи подписи всех пользователей сети конфиденциальной связи объединяются в справочники открытых ключей. Таким образом, каждому поль­зователю конфиденциальной сети, обладающему правом подпи­си, необходимо иметь закрытый ключ подписи и справочник от­крытых ключей.

Электронная цифровая подпись вырабатывается с помощью так называемой функции хэширования на основе элек­тронного документа, требующего заверения, и секретного ключа. Процесс выработки и использования электронной подписи за­ключается в следующем. На вход однонаправленной хэш-функ­ции поступает исходный документ произвольной длины. Хэш- функция преобразует его в хэш-значение фиксированной длины (например, 256 бит). Это значение однозначно зависит от содер­жания документа, но не позволяет восстановить сам документ. Затем полученное хэш-значение математически преобразуется в цифровую подпись электронного документа и передается вме­сте с документом. Хэш-функция обладает рядом уникальных свойств. Она чувствительна ко всевозможным изменениям в тек­сте, что позволяет их обнаружить; для данной хэш-функции практически нельзя подобрать два исходных разных сообщения, которые могут иметь одно и то же хэш-значение или одну и ту же цифровую подпись, т. е. подделать ее.

Для проверки электронной подписи необходимо знать от­крытый ключ пользователя, поставившего подпись. При про­верке снова вычисляется хэш-значение документа и проверя­ются некоторые соотношения, связывающие хэш-значение до­кумента, подпись под этим документом и открытый ключ подписавшего пользователя. Документ считается подлинным, а подпись правильной, если эти соотношения выполняются. В противном случае подпись под документом считается недей­ствительной.

Использование электронной подписи связано с вопросом подлинности открытых ключей. Для разрешения споров между отправителем и получателем информации, связанных с возмож­ностью искажения пересылаемого документа или открытого ключа проверки подписи, достоверная копия этого ключа мо­жет выдаваться третьей стороне (арбитру) и применяться им при возникновении конфликта между отправителем и получа­телем. Для контроля целостности и подлинности справочников открытых ключей используется процедура выработки имито- вставки.

**4. Криптографические стандарты *DES и ГОСТ 28147—89.*** Рас­смотрим кратко широко известные алгоритмы блочного шифро­вания, принятые в качестве государственных стандартов шифро­вания данных в США и России.

В 1973 г. Национальное бюро стандартов США начало разра­ботку программы по созданию стандарта шифрования данных на ЭВМ. Был объявлен конкурс среди фирм-разработчиков США, который выиграла фирма IBM, представившая в 1974 г. алго­ритм шифрования, известный под названием DES (Data Encryp­tion Standart).

В этом алгоритме входные 64-битовые векторы, называемые блоками открытого текста, преобразуются в выходные 64-бито- вые векторы, называемые блоками шифротекста, с помощью двоичного 56-битового ключа ***К.*** Число различных ключей DES-алгоритма равно 256 > 7 • 1016.

Алгоритм реализуется в течение 16 аналогичных циклов шифрования, где на ***i-м*** цикле используется цикловый ключ ***Kh*** представляющий собой алгоритмически вырабатываемую выбор­ку 48 битов из 56 битов ключа /= 1, 2, ..., 16.

Из-за небольшого размера ключа было принято решение ис­пользовать DES-алгоритм для закрытия коммерческой (несек­ретной) информации. Практическая реализация перебора всех ключей в данных условиях экономически нецелесообразна, так как затраты на реализацию перебора не соответствуют ценности информации, закрываемой шифром.

DES-алгоритм явился первым примером широкого производ­ства и внедрения технических средств в области защиты инфор­мации. Национальное Бюро Стандартов США проводит провер­ку аппаратных реализаций DES-алгоритма, предложенных фир­мами-разработчиками на специальном тестирующем стенде. Только после положительных результатов проверки производи­тель получает от Национального Бюро Стандартов сертификат на право реализации своего продукта. К настоящему времени атте­стовано несколько десятков изделий, выполненных на различной элементной базе.

Основные области применения DES-алгоритма:

* хранение данных в ЭВМ (шифрование файлов, паролей);
* аутентификация сообщений (имея сообщение и контроль­ную группу, несложно убедиться в подлинности сообщения);
* электронная система платежей (при операциях с широкой клиентурой и между банками);

• электронный обмен коммерческой информацией (обмен данными между покупателем, продавцом и банкиром за­щищен от изменений и перехвата).

В 1989 г. в СССР был разработан блочный шифр для ис­пользования в качестве государственного стандарта шифрова­ния данных. Разработка была принята и зарегистрирована как ГОСТ 28147—89. И хотя масштабы применения этого алгорит­ма шифрования до сих пор уточняются, начало его внедрению, в частности, в банковской системе, уже положено. Алгоритм, судя по публикациям, несколько медлителен, но обладает весь­ма высокой стойкостью.

Блок-схема алгоритма ГОСТ отличается от блок-схемы DES- алгоритма лишь отсутствием начальной перестановки и числом циклов шифрования (32 в ГОСТе против 16 в DES-алгоритме).

В шифре ГОСТ используется 256-битовый ключ, и объем ключевого пространства составляет 2256. Ни на одной из суще­ствующих в настоящее время или предполагаемых к реализации в недалеком будущем ЭВМ общего применения нельзя подоб­рать ключ за время, меньшее многих сотен лет. Российский стандарт проектировался с большим запасом, по стойкости он на много порядков превосходит американский стандарт DES с его реальным размером ключа в 56 бит и объемом ключевого пространства всего 256. В свете прогресса современных вычис­лительных средств этого явно недостаточно и в этой связи DES может представлять, скорее, исследовательский или научный, чем практический интерес.

Алгоритм расшифровки отличается от алгоритма зашифров­ки тем, что последовательность ключевых векторов используется в обратном порядке.

Расшифровка данных возможна только при наличии син- хропосылки, которая в скрытом виде хранится в памяти ЭВМ или передается по каналам связи вместе с зашифрованными данными.

Важной составной частью шифросистемы является ключевая система шифра. Под ней обычно понимается описание всех ви­дов ключей (долговременные, суточные, сеансовые и др.), ис­пользуемых шифром, и алгоритмы их использования (протоколы шифрованной связи) В электронных шифраторах в качестве ключей могут исполь­зоваться начальные состояния элементов памяти в схемах, реали­зующих алгоритм шифрования, функциональные элементы алго­ритма шифрования. Ключ может состоять из нескольких ключе­вых составляющих различных типов: долговременных, сеансовых и т. д.

Одной из основных характеристик ключа является его раз­мер, определяющий число всевозможных ключевых установок шифра. Если размер ключа недостаточно велик, то шифр может быть вскрыт простым перебором всех вариантов ключей. Если размер ключа чрезмерно велик, то это приводит к удорожанию изготовления ключей, усложнению процедуры установки ключа, понижению надежности работы шифрующего устройства и т. д. Таким образом, выбранный криптографом размер ключа — это всегда некий компромисс.

Заметим, что DES-алгоритм подвергался критике именно в связи с небольшим размером ключа, из-за чего многие крипто- логи пришли к мнению, что необходимым «запасом прочности» DES-алгоритм не обладает.

Другой важной характеристикой ключа является его случай­ность. Наличие закономерностей в ключе приводит к неявному уменьшению его размера и, следовательно, к понижению крип­тографической стойкости шифра. Такого рода ослабление крип­тографических свойств шифра происходит, например, когда ключевое слово устанавливается по ассоциации с какими-либо именами, датами, терминами Всякая логика в выборе ключа на­носит ущерб криптографическим свойствам шифра. Таким обра­зом, требование случайности ключей выступает как одно из ос­новных при их изготовлении.

Для изготовления ключей могут использоваться физические Датчики и псевдослучайные генераторы со сложным законом об­разования ключа. Использование хорошего физического датчика более привлекательно с точки зрения обеспечения случайности ключей, но является, как правило, более дорогим и менее про­изводительным способом. Псевдослучайные генераторы более дешевы и производительны, но привносят некоторые зависимо­сти, если не в отдельные ключи, то в совокупности ключей, что также нежелательно.

Важной частью практической работы с ключами является обеспечение секретности ключа. К основным мерам по защите ключей относятся следующие:

* ограничение круга лиц, допущенных к работе с ключами;

» регламентация рассылки, хранения и уничтожения ключей;

* регламентация порядка смены ключей;
* применение технических мер защиты ключевой информа­ции от несанкционированного доступа.

***RSA — криптографическая система открытого ключа,*** обес­печивает такие механизмы защиты как шифрование и цифровая подпись (аутентификация — установление подлинности). Крип­тосистема RSA разработана в 1977 г. и названа по инициалам ее разработчиков R. Rivest, A. Shamir и L. Adleman.

Вообще же, все предлагаемые сегодня криптосистемы с от­крытым ключом опираются на один из следующих типов необ­ратимых математических преобразований:

* разложение больших чисел на простые множители;
* вычисление логарифма в конечном поле;
* вычисление корней алгебраических уравнений.

Алгоритм RSA базируется на первом из этих принципов и

работает следующим образом: берутся два достаточно больших простых числа *р* и *q,* затем вычисляется их произведение *п = рх q* (называемое модулем).

Затем выбирается число е, которое удовлетворяет условию 1<е<(р-1)х(#-1)ине имеет общих делителей, кроме 1 (вза­имно простое) с числом *(р-* 1) х *(q -* 1). Затем вычисляется чис­ло *d* таким образом, что *(ed-* 1) делится на (р- 1) х {q- 1). Та­ким образом, здесь:

е — открытый (public) показатель;

*d —* частный (private) показатель;

(л; е) — открытый (public) ключ;

(«; d) — частный (private) ключ.

Делители (факторы) *р* и *q* можно либо уничтожить, либо со­хранить вместе с частным (private) ключом.

Если бы существовали эффективные методы разложения на сомножители (факторинга), то, разложив п на сомножители (факторы) *р* и *q,* можно было бы получить частный (private) ключ *d.* Таким образом, надежность криптосистемы RSA осно­вана на практически неразрешимой задаче разложения п на со­множители (т. е. на невозможности факторинга п), так как в на­стоящее время эффективного способа поиска сомножителей не существует.

Криптосистема RSA используется в самых различных про­дуктах, на различных платформах и во многих отраслях. В на­стоящее время криптосистема RSA встраивается во многие ком­мерческие продукты, число которых постоянно увеличивается.

Также ее используют операционные системы Microsoft, Apple, Sun и Novell. В аппаратном исполнении RSA алгоритм приме­няется в защищенных телефонах, на сетевых платах Ethernet, на смарт-картах, широко используется в криптографическом обо­рудовании. Кроме того, алгоритм входит в состав всех основных протоколов для защищенных коммуникаций Internet, в том чис­ле S/MIME, SSL и S/WAN, а также используется во многих уч­реждениях, например, в правительственных службах, в боль­шинстве корпораций, в государственных лабораториях и уни­верситетах.

Криптосистема RSA — часть многих стандартов. Стандарт ISO 9796 описывает RSA как совместимый криптографический алгоритм, соотвествующий стандарту безопасности ITU-T Х.509. Кроме этого криптосистема RSA является частью стандартов SWIFT, ANSI Х9.31 rDSA и проекта стандарта Х9.44 для амери­канских банков. Австралийский стандарт управления ключами AS2805.6.5.3 также включает систему RSA.

Алгоритм RSA используется в Internet, в частности он входит в такие протоколы, как S/MIME, IPSEC (Internet Protocol Security) и TLS (которым предполагается заменить SSL), а также в стандарт PKCS, применяемый в важных приложениях.

**Литература**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2011
3. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
4. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
5. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.intuit.ru](http://www.intuit.ru).
* [www.garant.ru](http://www.garant.ru)