**Вопросы к экзамену «Организационное и правовое обеспечение информационной безопасности»**

**Модуль 1: Организационное и правовое обеспечение информационной безопасности (Струков В.И.)**

1. **Структура информационного законодательства в РФ. Органы, обеспечивающие информационную безопасность в РФ.**

**Информационное законодательство** — это совокупность норм права, регулирующих общественные отношения в информационной сфере.

**Структура информационного законодательства РФ:**

* Международные акты информационного законодательства, начиная с Всеобщей декларации прав человека от 10.12.1948г.
* Конституция РФ
* Гражданский кодекс РФ, Уголовный кодекс РФ и др. кодексы.
* Законы РФ: “Об информации, информационных технологиях и о защите информации”, “О государственной тайне”, “О коммерческой тайне”, “О персональных данных”, “Об электронной подписи” и др. (всего около 80 законов)
* Указы и Распоряжения Президента РФ. Постановления Правительства РФ.
* Местные, ведомственные и внутриорганизационные подзаконные акты.

**Органы, обеспечивающие информационную безопасност**ь: Правительство РФ, Совет безопасности РФ, Федеральная служба безопасности РФ (ФСБ), Служба специальной связи и информации при Федеральной службе охраны РФ, Федеральная служба по техническому и экспортному контролю РФ (ФСТЭК), Государственная фельдъегерская служба РФ, Межведомственная комиссия по защите государственной тайны.

***(СОВСЕМ НЕ ОБЯЗАТЕЛЬНО)*** *В зависимости от приложения деятельности в области защиты информации (в рамках государственных органов власти или коммерческих организаций), сама деятельность организуется специальными государственными органами (описаны выше), либо отделами (службами) предприятия.*

***Службы, организующие защиту информации на уровне предприятия:*** *служба экономической безопасности; служба безопасности персонала (Режимный отдел); отдел кадров; служба информационной безопасности.*

1. **Место информационного права в системе права. Свойства информационного товара.**

**Система права** – совокупность всех нормативно-правовых актов**.** Внутреннее строение права можно представить по вертикали и горизонтали.

**Вертикальное строение права** — это совокупность следующих элементов:

* Отрасль права - охватывает сферу общественных отношений. *Например, имущественные отношения - гражданское право, управленческие отношения - административное право, и т.п.*
* Подотрасль права - охватываетобласть общественных отношений. Многие отрасли права имеют подотрасли. *Например, в гражданском праве выделяются подотрасли - авторское и наследственное право.*
* Институт права - охватывает вид общественных отношений. *В трудовом праве - институт трудового договора.*
* Субинститут права - охватывает разновидность общественных отношений. *Институт преступлений против жизни, здоровья, достоинства личности.*
* Норма права — это обязательное правило поведения, охраняемое силой государственного принуждения.
* Правовое предписание — это часть нормы права, логически завершенная и обособленная. *Размер алиментов, взыскиваемых на одного ребенка (25 % заработка), на двух (33 %), на трех и более (50 %).*

**Горизонтальное строение права** показывает все отрасли, его составляющие. Всего выделяют две группы отраслей регулятивные и охранительные.

Регулятивные отрасли устанавливают права и обязанности участников правоотношений. Это следующие отрасли: конституционное право, административное право, гражданское право, финансовое право, банковское право, предпринимательское право, трудовое право, природоресурсное право, экологическое право, информационное право.

Охранительные отрасли права*:* уголовное право, уголовно-процессуальное право, уголовно-исполнительное право, гражданско-процессуальное право, арбитражно-процессуальное право

**Свойства информационного товара:** Нематериальность; Неисчерпаемость; Сохраняемость; Цена; Потребительские свойства; Жизненный цикл информации

1. **Предмет правового регулирования в информационной сфере. Юридическая ответственность за нарушения правовых норм в информационной сфере.**

**Основным предметом правового регулирования информационного права** выступает информация, то есть общественные отношения в информационной сфере, возникающие при осуществлении информационных процессов — процессов производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления информации

**Предметы правового регулирования** в информационной сфере:

* создание и распространение информации;
* формирование информационных ресурсов;
* реализация права на поиск, получение, передачу и потребление информации;
* создание и применение информационных систем и технологий;
* создание и применение средств информационной безопасности.

Нормативно-правовое регулирование отношений в области защиты информации осуществляется информационным правом, которое является одним из составляющих существующей системы права.

**Юридическая ответственность подразделяется по отраслевому признаку:**

* Уголовная ответственность наступает за совершение преступлений и устанавливается только уголовным законом.
* Административно-правовая ответственность наступает за совершение административных проступков. Меры административного принуждения - предупреждение, штраф, лишение специального права, административный арест.
* Гражданско-правовая ответственность наступает за нарушения договорных обязательств имущественного характера или за причинение имущественного внедоговорного вреда. (Возмещение убытков, выплата неустойки).
* Дисциплинарная ответственность возникает вследствие совершения дисциплинарных проступков. Меры дисциплинарной ответственности - выговор, строгий выговор, отстранение от занимаемой должности и т.п.
* Материальная ответственность рабочих и служащих за ущерб, нанесенный предприятию, учреждению. Размер возмещаемого ущерба определяется в процентах к заработной плате (1/3, 2/3 месячного заработка).

1. **Основные положения закона РФ «Об информации…». Методы защиты информации.**

***Закон РФ “Об информации, информационных технологиях и о защите информации” от 27.13.2006г. № 149-Ф3*** регулирует следующие отношения:

* осуществление права на поиск, получение, передачу, производство и распространение информации;
* ограничение доступа к информации;
* применение информационных технологий.

**В законе раскрыты следующие важные вопросы:**

* Основные понятия в области информации, и ее защиты.
* Права обладателя информации.
* Право на доступ и ограничения доступа к информации.
* Использование информационно-телекоммуникационных сетей и государственное регулирование в этой сфере.
* Защита информации, в том числе использование ЭЦП.

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

* обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* соблюдение конфиденциальности информации ограниченного доступа,
* реализацию права на доступ к информации.

**На практике используют несколько групп методов защиты, в том числе:**

* препятствие на пути предполагаемого похитителя, которое создают физическими и программными средствами;
* управление, или оказание воздействия на элементы защищаемой системы;
* маскировка, или преобразование данных, обычно – криптографическими способами;
* регламентация, или разработка нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;
* принуждение, или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;
* побуждение, или создание условий, которые мотивируют пользователей к должному поведению.

1. **Режимы доступа к информации. Информация свободного доступа. Виды режимов ограниченного доступа.**

**Режим государственной тайны** устанавливается в соответствии с законом РФ “О государственной тайне”. **Режим конфиденциальности** устанавливается в отношении сведений, перечисленных в Указе Президента РФ № 188 от 6.03.1997г. (ред. от 23.09.2005 №1111) и регулируется законами: “О коммерческой тайне”, “О персональных данных”, “О связи”, “О банках и банковской деятельности”, “О милиции” и др.

Информация (в зависимости от порядка распространения) **подразделяется на**: свободно распространяемую; предоставляемую по соглашению; распространяемую в соответствии с федеральными законами; распространение которой в РФ ограничивается или запрещается.

К **общедоступной информации** относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация **может использоваться** любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. **Запрещается** распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, и т.п.

**Общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или в соответствии с федеральными законами.

**Перечень сведений**, доступ к которым **не подлежит** какому–либо ограничению:

* нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
* информация о состоянии окружающей среды;
* информация о деятельности государственных органов и органов местного самоуправления (за исключением сведений, составляющих государственную или служебную тайну);
* информация, в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных для обеспечения граждан и организаций такой информацией;
* информация, недопустимость ограничения доступа к которой установлена федеральными законами.

**Свободный доступ:** Общественного достояния (научные открытия, рукописи и т.п.); Массовой информации (Информация в СМИ, различные публикации и т.д.); Исключительных прав (Результаты интеллектуальной деятельности).

**Ограниченный доступ:** Конфиденциальности (Коммерческая, служебная и профессиональная тайны. Персональные данные. Тайна следствия и судопроизводства. Сведения о сущности неопубликованных изобретений); Государственной тайны (Секретно, совершенно секретно и особой важности)

1. **Режим исключительных прав. Формы правовой защиты интеллектуальной собственности.**

**Исключительное право** — совокупность принадлежащих правообладателю (гражданину или юридическому лицу) прав на использование по своему усмотрению любым не противоречащим закону способом результата интеллектуальной деятельности или средства индивидуализации и на запрещение или разрешение такого использования другими лицами.

Правообладатель **может распоряжаться** исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации, если законом не предусмотрено иное.

Правообладатель **вправе** по своему усмотрению разрешать или запрещать другим лицам использование результата интеллектуальной деятельности или средства индивидуализации. Отсутствие запрета не считается согласием (разрешением).

Использование результата интеллектуальной деятельности или средства индивидуализации, если такое использование осуществляется без согласия правообладателя, является незаконным и влечет ответственность, установленную Гражданским кодексом РФ, другими законами, за исключением случаев, когда использование результата интеллектуальной деятельности или средства индивидуализации лицами иными, чем правообладатель, без его согласия допускается Гражданским кодексом РФ.

**Исключительное право** на результат интеллектуальной деятельности или на средство индивидуализации (кроме исключительного права на фирменное наименование) может принадлежать одному лицу или нескольким лицам совместно.

**Существует** правовые формы защиты интеллектуальной собственности:

* авторское право, ([ст. 146](https://student2.consultant.ru/cgi/online.cgi?req=doc&base=LAW&n=405601&dst=102318) УК РФ)
* патентное право, ([ст. 147](https://student2.consultant.ru/cgi/online.cgi?req=doc&base=LAW&n=405601&dst=100832) УК РФ);
* секреты производства - «ноу-хау». (ст. 1465 ГК РФ)
* товарные знаки и знаки обслуживания, наименование места происхождения товара ([ст. 180](https://student2.consultant.ru/cgi/online.cgi?req=doc&base=LAW&n=405601&dst=1755) УК РФ).

Режим исключительных прав определен ***Гражданским кодексом РФ, часть 4, от 18.12.2006г. № 230.***

Истечение срока действия исключительных прав на объекты интеллектуальной собственности (например, **авторское право** действует в течение всей жизни автора и 70 лет после его смерти) означает переход их в общественное достояние.

1. **Конфиденциальность информации. Перечень сведений конфиденциального характера.**

**Режим конфиденциальности** устанавливается в отношении сведений, перечисленных в ***Указе Президента РФ № 188 от 6.03.1997г.*** *(ред. от 23.09.2005 №1111)* и регулируется законами: **“*О коммерческой тайне”, “О персональных данных”, “О связи”, “О банках и банковской деятельности”, “О милиции” и др.***

Режим конфиденциальной информации по данным законодательных и подзаконных актов в настоящее время включает более 50 видов тайн. Указом Президента РФ № 188 от 6.03.1997г. утвержден перечень сведений конфиденциального характера:

1. Коммерческая тайна
2. Служебная тайна
3. Профессиональная тайна (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
4. 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.
5. Тайна следствия и судопроизводства
6. Сведения о сущности неопубликованных изобретений
7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными (в соответствии с Федеральным [законом](https://www.consultant.ru/document/cons_doc_LAW_436660/1c194590ac1e7f7d1f67e084b018deaae29bcdef/#dst31) "Об исполнительном производстве".)

**Конфиденциальность персональных данных** – обязательное требование не допускать их распространение без согласия субъекта персональных данных или законного основания.

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.

1. **Требования по безопасности компьютерных сетей в РФ.**

**Требования по безопасности компьютерных сетей** разработаны ГТК РФ («Государственный таможенный комитет Российской Федерации») и **обязательны** для государственных предприятий или для коммерческих предприятий допущенных к сведениям составляющих ГТ. В остальных случаях они носят рекомендательный характер.

К таким документам относится, например, РД ГТК («Руководящий документ Гостехкомиссии») «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» от 30.03.92.

Установленные классы регламентируют использование в АС **следующих подсистем:** управления доступом; регистрации и учета; криптографической; обеспечения целостности.

Требования к безопасности АС устанавливаются в соответствии с классом защищенности. Установлено **9 классов** защищенности в трех группах:

**Третья группа:** АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности: **3A** информация, составляющая гостайну; **3Б** служебная тайна или персональные данные

**Вторая группа:** АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности: **2A** информация, составляющая гостайну; **2Б** служебная тайна или персональные данные

**Первая группа:** Многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС:

АС, в которых циркулирует информация, составляющая гостайну: 1А, 1Б и 1В.

* **1А** - в случае обработки секретной информации с грифом «особая важность»
* **1Б** - в случае обработки секретной информации с грифом не выше «совершенно секретно»
* **1В** - в случае обработки секретной информации с грифом не выше «секретно»
* **1Г** - АС, в которых циркулирует служебная тайна
* **1Д** - АС, в которых циркулируют персональные данные

Показатели защищенности средств вычислительной техники от НСД («Несанкционированный доступ») даны в РД ГТК «Средства ВТ. Защита от НСД. Показатели защищенности от НСД к информации» от  
30.03.92. В данном РД определяется 7 классов защищенности СВТ («Средства вычислительной техники») от НСД к информации. Классы подразделяются на **4 группы**:

* **Первая группа** содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов (Минимальная защита);
* **Вторая группа** характеризуется дискреционной защитой и содержит шестой и пятый классы (Избирательная защита, соответствие «субъект-объект»);
* **Третья группа** характеризуется мандатной защитой и содержит четвертый, третий и второй классы (Полномочная защита, наличие диспетчера доступа);
* **Четвертая группа** характеризуется верифицированной защитой и включает только первый класс.

Для присвоения класса защищенности АС **должна иметь**: руководство администратора по системе; руководство пользователя; тестовую и конструкторскую документацию.

1. **Правовая система защиты государственных секретов. Сведения, составляющие государственную тайну.**

Система защиты государственных секретов основывается на ***Законе РФ «О государственной тайне»*** *от 21.07.93г. №5485-1 (ред. 11 ноября 2003г. №153).* Закон регулирует отношения, связанные с отнесением сведений к государственной тайне (ГТ), их рассекречиванием и защитой в интересах безопасности РФ.

В законе даны следующие определения:

* **Государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно- розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.
* **Носители сведений, составляющих ГТ –** материальные объекты, в том числе физические поля, в которых сведения, составляющие ГТ, находят свое отображение в виде **символов,** **образов,** **сигналов,** **технических решений и** **процессов.**
* **Система защиты государственной тайны –** совокупность органов защиты ГТ используемых **средств** и **методов защиты** сведений, составляющих ГТ, и их **носителей**, а также **мероприятий**, проводимых в этих целях.

Перечень сведений, отнесенных к ГТ, утвержден ***Указом Президента РФ от 30.11.95г. №1203 (уточнен Указом Президента РФ от 11.02.2006 № 90).* [118 пунктов]**

В частности, в сферах экономики, науки и техники к государственной тайне **относятся** сведения:

* о научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение;
* о методах и средствах защиты секретной информации;
* о государственных программах и мероприятиях в области защиты государственной тайны.
* сведения, раскрывающие план применения Вооруженных Сил Российской Федерации, оперативные планы применения (планы боевого применения) войск, содержание мероприятий, касающихся военных действий и их обеспечения, боевого управления или перевода с мирного на военное время, а также боевые задачи носителям ядерного оружия.
* сведения, раскрывающие планы применения войск в мирное время в специальных (контртеррористических) операциях или мероприятиях по обеспечению защиты государства, общества и личности от антиконституционных действий и противоправного вооруженного насилия.
* сведения об использовании инфраструктуры Российской Федерации в интересах обеспечения обороноспособности и безопасности государства.
* сведения о силах или средствах гражданской обороны.

Устанавливаются три степени секретности сведений, составляющих ГТ, и соответствующие **грифы секретности** для носителей указанных сведений:

* "особой важности" (ОВ) – если при разглашении наносится ущерб интересам РФ;
* "совершенно секретно" (СС) – если при разглашении наносится ущерб интересам  
  отрасли или министерства;
* "секретно" (С) – если при разглашении наносится ущерб интересам  
  предприятия.

Существует также промежуточный гриф для документов, которые не являются тайной предприятия, но не предназначены для открытого использования: **ДСП** – для служебного пользования.

1. **Степени секретности сведений, составляющих государственную тайну. Принципы засекречивания и порядок рассекречивания сведений, составляющих государственную тайну.**

Правила, по которым определяется степень секретности сведений, представляющих ГТ утверждены ***Постановлением Правительства РФ №870 от 04.09.95г.***

Устанавливаются **три степени секретности** сведений, составляющих ГТ, и соответствующие грифы секретности для носителей указанных сведений:

* "особой важности" (ОВ) – если при разглашении наносится ущерб интересам РФ;
* "совершенно секретно" (СС) – если при разглашении наносится ущерб интересам отрасли или министерства;
* "секретно" (С) – если при разглашении наносится ущерб интересам предприятия.

Порядок засекречивания сведений, составляющих ГТ, основан на **трех принципах**:

1. Законности. Заключается в том, что засекречиванию не подлежат сведения, указанные в статье 7 закона о ГТ (которые раньше относились к ГТ).
2. Обоснованности. Заключается в установлении целесообразности засекречивания сведений по экономическим или иным критериям.
3. Своевременности. заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

**Не подлежат отнесению** к государственной тайне и засекречиванию сведения:

* о чрезвычайных происшествиях и катастрофах;
* о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
* о привилегиях и льготах гражданам, должностным лицам, предприятиям;
* о фактах нарушения прав и свобод человека и гражданина;
* о состоянии здоровья высших должностных лиц;
* о фактах нарушения законности органами государственной власти и их должностными лицами.

***Постановлением Правительства РФ №170 от 20.02.95г*** установлен **порядок рассекречивания** и продления сроков засекречивания архивных документов. Основания для рассекречиваниясведений:

* взятие на себя РФ международных обязательств по открытому обмену сведениями, составляющими ГТ;
* изменение обстоятельств, вследствие чего дальнейшая защита сведений является нецелесообразной.

Органы государственной власти обязаны **каждые 5 лет** пересматривать содержание действующих перечней. Срок засекречивания сведений, составляющих ГТ, не должен превышать **30 лет**. В исключительных случаях этот срок может быть продлен по заключению межведомственной комиссии по защите ГТ. Носители сведений, составляющих ГТ, рассекречиваются не позднее сроков, установленных при их засекречивании. Органы защиты государственной тайны: ФСБ, МО, СВР, ФСТЭК.

1. **Условия допуска юридических и физических лиц к ГТ. Ответственность за разглашение информации, содержащей государственную тайну.**

Допуск должностных лиц и граждан к ГТ **предусматривает**:

* принятие на себя обязательствперед государством по нераспространению сведений, составляющих ГТ;
* согласие на частичные, временные ограничения их правв соответствии со статьей 24 настоящего Закона;
* письменное согласие на проведениев отношении их полномочными органамипроверочных мероприятий;
* определение видов**,** размеров и порядка предоставленияльгот**,** предусмотренных настоящим Законом;
* ознакомление с нормами законодательстваРФ о ГТ, предусматривающими ответственность за его нарушение;
* принятие решенияруководителем органа государственной власти или предприятия, одопуске лица к сведениям, составляющим ГТ.

Устанавливаются **три формы допуска** к ГТ должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих ГТ: **Первая** – к сведениям "особой важности" (ОВ); **Вторая** – к сведениям "совершенно секретно" (СС); **Третья** – к сведениям "секретно" (С).

**Сроки, обстоятельства и порядок переоформления допуска** граждан к ГТ устанавливаются нормативными документами Правительством РФ.

**Особый порядок допуска** к ГТ имеют: Члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, адвокаты, участвующие в уголовном судопроизводстве по делам, связанным со сведениями, составляющими ГТ. Эти лица допускаются к сведениям, составляющим ГТ, без проведения проверочных мероприятий.

**Ответственность за организацию защиты сведений**, составляющих ГТ, в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей. Должностные лица и граждане, виновные в нарушении законодательства РФ о ГТ, **несут** уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

Уголовно-правовая ответственность за разглашение информации, содержащей ГТ, определяетсяУголовным кодексом РФ **- Статья 275 Государственная, Статья 276. Шпионаж**, **Статья 283. Разглашение государственной тайны**, **Статья 284. Утрата документов, содержащих ГТ**.

1. **Сведения, составляющим КТ. Виды конкурентной разведки.**

К **коммерческой тайне** относят следующие три группы сведений:

* **Деловая информация** (о сферах деятельности): финансовые сведения; данные о себестоимости продукции и услуг; деловые планы и планы производства и развития; информация о маркетинге; соглашения, предложения, контракты; организационные схемы.
* **Техническая информация:** научно-исследовательские проекты; конструкторская документация на продукцию; заявки на патенты; дизайн, передовые технологии и оборудование; программное обеспечение ЭВМ и информационный процесс; химические формулы.
* **Информация о клиентах и конкурентах.** На каждого клиента фирмы накапливается информация, где отражаются его привычки, характерные черты поведения, интересы в личной жизни, о представляемых ему фирмой привилегиях и т. п. Аналогичные базы данных составляют и на своих конкурентов.Таким образом, формируются **«профиль клиента»** и **«профиль конкурента»**.

Существует **три основных направления сбора информации,** представляющей коммерческий интерес:

* Информация о рынке (издается и публикуется)
* Информация о производстве продукции (закупки, наблюдение, опрос)
* Информация об организационных особенностях и планах развития

**Сведения о деятельности фирмы и ее руководителях** собирают в различных экономических газетах и журналах, справочниках, выписывают у биржевиков, покупают у частных детективов, а также с помощью конкурентной разведки через Интернет. Принято **различать**: конкурентную разведку ("деловая разведка", "бизнес-разведка") и промышленный шпионаж. **Отличие** заключается в соблюдении закона в первом случае и нарушениях уголовного, авторского или любого другого права – во втором.

**Конкурентная разведка** – это сбор и обработка информации законными способами. На данный момент в нашей стране под конкурентной разведкой подразумеваются четыре вида сбора информации:

* Сбор данных о партнерах и клиентах для предотвращения мошенничеств с их стороны.
* Информация о потенциальных партнерах и сотрудниках. Обычно этим занимаются отделы безопасности компаний или частные детективные агентства
* Выполнение услуг охраны и сыска, предусмотренных Законом "О частной детективной и охранной деятельности ".
* Сбор информации маркетингового характера.

**Виды конкурентной разведки** (сбор информации маркетингового характера): наблюдение; отчеты торговых работников; поиск информации в открытых БД; анализ годовых отчетов предприятий; обратный инжиниринг.

В настоящее время получила широкое распространение конкурентная разведка через Интернет. Выделяют **три режима такой разведки**: оперативный (сбор и предоставление информации за 10 мин.)‏; ситуационный центр (подготовка информации руководству с выводом на экран за 3–4 часа); оперативные исследования (проведение исследований и подготовка отчета за 1–2 дня).

1. **Правовая защита коммерческой тайны. Сведения, которые не могут составлять КТ.**

Для обозначения степени важности коммерческой информации для предприятия можно предложить систему обозначения степени ее секретности:

1. Коммерческая тайна – строго конфиденциально (КТ-СК)
2. Коммерческая тайна – конфиденциально (КТ-К)
3. Коммерческая тайна (КТ)

***Закон "О коммерческой тайне" 29 июля 2004 года N 98*** регулирует отношения, связанные с отнесением информации к КТ, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестной конкуренции, а также определяет сведения, которые не могут составлять КТ.

**КТ** – **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 (ст. 3).

**Режим коммерческой тайны -** правовые, организационные, технические и иные меры по охране ее конфиденциальности. Не могут составлять КТ (ст. 5) сведения:

* содержащие в учредительных документах юридического лица, и индивидуальных предпринимателях;
* дающие право на осуществление предпринимательской деятельности;
* о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
* о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической обстановке и других факторах;
* 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;
* о нарушениях законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений;
* об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
* 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;
* о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
* о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
* сведения, недопустимость ограничения доступа к которым установлена иными федеральными законами.

Обладатель информации, составляющей КТ, по требованию органа государственной власти предоставляет ее на безвозмездной основе (ст. 6).

1. **Мероприятия, необходимые для введения режима КТ на предприятии. Ответственность за разглашение КТ.**

**Режим коммерческой тайны -** правовые, организационные, технические и иные меры по охране ее конфиденциальности. Режим КТ, считается установленным, после принятия обладателем информации **следующих мер:**

* определение перечня информации, составляющей КТ;
* ограничение доступа к информации, составляющей КТ, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
* учет лиц, получивших доступ к информации, составляющей КТ, и (или) лиц, которым такая информация была предоставлена или передана;
* регулирование отношений по использованию информации, составляющей КТ, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
* нанесение на документы, содержащие КТ, грифа **"Коммерческая тайна"** и обладателя этой информации. **Для юридических лиц** - полное наименование и место нахождения; **для индивидуальных предпринимателей** — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства.
* ознакомитьпод расписку работника с перечнем информации, составляющей КТ;
* создать работнику необходимые условия для соблюдения им установленного работодателем режима КТ;
* ознакомить под расписку работника с установленным работодателем режимом КТ и с мерами ответственности за его нарушение.

**Доступ работника к информации**, составляющей КТ, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями. В случае нарушения конфиденциальности информации должностными лицами органов государственной власти эти лица несут ответственность в соответствии с законодательством РФ (ст. 13).

**Ответственность за нарушение настоящего закона** (ст. 14). Нарушение закона влечет за собой: дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

Органы государственной власти, несут гражданско-правовую ответственность за разглашение или незаконное использование КТ их должностными лицами, которым она стала известна в связи с выполнением ими должностных обязанностей (ст. 14). Лицо, которое использовало информацию, составляющую КТ, и не имело достаточных оснований считать использование данной информации незаконным, (получило доступ к ней в результате случайности или ошибки), не может быть привлечено к ответственности (ст. 14).

1. **Внутрифирменные документы, используемые для регулирования правовых отношений по защите КТ на предприятии. Правовая защита электронных документов.**

В соответствии с установленными законом о КТ на предприятии **используются правовые нормы** внутрифирменных документов для регулирования правовых отношений по защите КТ. Такими документами **являются:** устав предприятия; коллективный договор предприятия; трудовые и гражданско-правовые договора; правила внутреннего трудового распорядка рабочих и служащих предприятия; должностные обязанности руководителей, специалистов, рабочих и служащих предприятия и другие документы.

**Электронный документ** должен создаваться, обрабатываться, храниться и передаваться с помощью электронных технических средств с соблюдением необходимой степени защиты, позволяющей гарантировать предотвращение несанкционированных воздействия, разглашения и доступа к защищенной информации с целью ее уничтожения, модификации, искажения, копирования, блокирования, предусмотренной действующим законодательством Российской Федерации, государственными или международными стандартами либо соглашением сторон.

**Все персональные данные**, к которым стороны имеют доступ в рамках осуществления электронного документооборота, должны быть защищены необходимыми гарантиями сохранения конфиденциальности персональных данных согласно действующему законодательству Российской Федерации.

Каждая сторона обязана соблюдать процедуры и предпринимать меры по защите от несанкционированного доступа к электронным документам.

При хранении электронного документа **должна сохраняться** информация, которая позволяет установить происхождение и назначение электронного документа, а также дату и время его отправления или получения.

1. **Виды угроз информации в автоматизированных системах. Ответственность за компьютерные преступления.**

**Виды угроз информации** в автоматизированных системах:

* Перехват информации: по электромагнитному излучению; по виброакустическому каналу; видеоперехват; использование отходов информационного процесса.
* Несанкционированный доступ (НСД) к информации: физическое проникновение; установка шлейфов; подключение к линии связи законного пользователя; подбор кода доступа в т.ч. с помощью программ «взломщиков», в ручную с помощью «интеллектуального» перебора.
* Манипуляция данными и управляющими командами: умышленное изменение данных; изменение логических связей в электронных цепях и топологии микросхем.
* Компьютерные вирусы: троянский конь; троянский червь; логическая бомба; воздушный змей.
* Использование специальных программных средств: «моделирование» процессов и способов преступления путем создания игровой программы защита-преодоление.
* Использование двух или более способов и их комбинирование.

**Предметом правового регулирования** в информационной сфере **являются:** создание и распространение информации; формирование и использование информационных ресурсов; реализация права на поиск, получение, передачу и потребление информации; создание и применение информационных систем и технологий; создание и применение средств информационной безопасности.

**Ответственность**, возлагаемая в случаях правонарушений в информационной сфере, формулируется в различных нормативных правовых актах. Конкретные нормы, устанавливающие ответственность за нарушения сосредоточены в Уголовном, Гражданском, Административном кодексах и в др. правовых актах. Уголовное право регулирует отношения в области наиболее опасных правонарушений – преступлений.

1. **Правовые основы деятельности частных СБ. Лицензирование частной детективной и охранной деятельности. оружие и специальные средства частных охранников.**

**Служба безопасности (СБ) фирмы** — это самостоятельное структурное подразделение, которое решает задачи обеспечения защиты жизненно важных интересов фирмы в условиях коммерческого риска и конкурентной борьбы.

**Задачи службы безопасности:**

* Определение сведений, составляющих КТ; лиц, имеющих к ним доступ; предприятий-партнеров, на которых возможна утечка общих секретов.
* Выявление лиц и предприятий, проявляющих интерес к КТ предприятия.
* Разработка системы защиты документов с грифом КТ.
* Определение уязвимых участков на предприятии, аварии или сбои в работе которых могут нанести урон предприятию.
* Планирование, обоснование и организация мероприятий по защите экономической информации (техническое оснащение, подготовка кадров).
* Взаимодействие с ОВД.

**Служба безопасности** должна быть готова к возникновению кризисных ситуаций, этим занимается кризисная группа.

**Кризисной группой** разрабатываются следующие виды планов действий: при угрозе взрыва; при захвате заложников или похищения сотрудников фирмы; при вымогательстве; при нападении на сотрудников и помещения фирмы; при природных и техногенных катастрофах и т.п.

**Основным документом**, регулирующим вопросы создания и деятельности СБ, является Закон РФ «О частной детективной и охранной деятельности».

Предоставление лицензий на осуществление частной охранной деятельности производится органами внутренних дел. Лицензия предоставляется сроком на пять лет и действует на всей территории Российской Федерации. В лицензии указывается (указываются) вид (виды) охранных услуг, которые может оказывать лицензиат. Решение о предоставлении либо об отказе в предоставлении лицензии принимается в срок не более сорока пяти дней.

В ходе осуществления частной детективной деятельности **разрешается применять** специальные средства, а при осуществлении частной охраной деятельности –специальные средства и огнестрельное оружие только в случаях и в порядке, предусмотренных настоящим Законом.

**Перечень видов специальных средств**, используемых группой охраны СБ в соответствии с данным законом и Постановлением Правительства от 14.8.1992 N 587: жилет защитный; шлем защитный; спецсредство «Черемуха» и его аналоги; газовый пистолет; наручники; палка резиновая (пластиковая).

**Виды вооружения охранников**, (порядок приобретения, учета, хранения и ношения оружия регламентируются Правительством РФ): 9мм пистолет; ружье охотничье гладкоствольное; боеприпасы к оружию.

На частную детективную и охранную деятельность распространяются правила применения специальных средств, установленные Правительством РФ для органов внутренних дел. Частные детективы и охранники **имеют право применять**:

* специальные средства в следующих случаях: для отражения нападения или для пресечения преступления, когда правонарушитель оказывает физическое сопротивление.
* огнестрельное оружие: для отражения нападения; для предупреждения (выстрелом в воздух).

1. **Виды услуг, разрешенных частным детективам и охранникам. Правовая ответственность за превышение ими своих полномочий.**

В целях сыска разрешается предоставление следующие **7 видов услуг**:

* сбор сведений по гражданским делам;
* изучение рынка, сбор информации для деловых переговоров, выявление некредитоспособных или ненадежных деловых партнеров;
* установление фактов недобросовестной конкуренции, а также разглашения сведений, составляющих коммерческую тайну;
* выяснение биографических и других данных об отдельных гражданах (с их письменного согласия) при заключении ими трудовых и иных контрактов; поиск без вести пропавших граждан; поиск утраченного имущества;
* сбор сведений по уголовным делам на договорной основе с участниками процесса.

В течение суток с момента заключения контракта с клиентом на сбор таких сведений частный детектив обязан письменно уведомить об этом следователя, прокурора или суд, в чьем производстве находится уголовное дело.

В целях охраны разрешается предоставление следующих **5 видов услуг**:

* защита жизни и здоровья граждан;
* охрана имущества собственников;
* проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации;
* консультирование клиентов по вопросам защиты от противоправных посягательств;
* обеспечение порядка в местах проведения массовых мероприятий.

Частным детективам **запрещается:**

* выдавать себя за сотрудников правоохранительных органов;
* осуществлять видео- и аудиозапись, фото- и киносъемку в служебных или иных помещениях без письменного согласия на то соответствующих должностных или частных лиц;
* проведение сыскных действий, нарушающих тайну переписки, телефонных переговоров и телеграфных сообщений либо связанных с нарушением гарантий неприкосновенности личности или жилища;
* скрывать от правоохранительных органов ставшие им известными факты готовящихся, совершаемых или совершенных преступлений;
* разглашать сведения, касающиеся вопросов обеспечения защиты жизни и здоровья граждан и (или) охраны имущества заказчика;
* получать и использовать информацию органов, осуществляющих оперативно-розыскную деятельность; использовать методы сыска.

**Ответственность за превышение полномочий** (УК РФ. Статья 203): Совершение частным детективом или работником частной охранной организации действий, выходящих за пределы полномочий, установленных законодательством РФ, и повлекших существенное нарушение прав и законных интересов граждан, организаций или государства, – **наказывается штрафом** в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо **ограничением свободы** на срок до двух лет, либо **лишением свободы** на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет.

1. **Правовое обеспечение использования технических средств съема и защиты информации. Ответственность за незаконное использование СТС.**

К техническим средствам сбора информации **относятся:**

* Основные технические средства: телефоны городской, внутренней и сотовой связи; селекторная связь; ПК и сети ПЭВМ; копировальная техника.
* Вспомогательные технические средства и системы: телевизор, магнитофон и др. виды бытовой радиоэлектроники; датчики охраны и пожарной сигнализации; кондиционер; штатное электрооборудование и сети газификации помещения.
* Специальные технические средства сбора информации: Радиомикрофон (жучок); Стетоскоп; Лазерный локатор; Направленный микрофон; Миниатюрные видео- и фотокамеры; Оборудование для приема побочного ЭМ излучение элементов ПК; Оборудование для прослушивания каналов мобильной связи.

**Правовая защита информации**, циркулирующей в телефонных и др. линиях связи:

* Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.
* Ограничение этого права допускается только на основании судебного решения.
* Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается.

Согласно **закону УК РФ Статья 138.1** *«Незаконный оборот специальных технических средств, предназначенных для негласного получения информации»* незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для негласного получения информации, – **наказываются штрафом** в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо **ограничением свободы** на срок до четырех лет, либо **принудительными работами** на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо **лишением свободы** на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

1. **Лицензирование и контроль в области СТС получения информации. Виды деятельности, подлежащие лицензированию в области СТС.**

Постановлением Правительства от 01.07.96г. №770 введено *“Положение о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в РФ и вывоза за ее пределы СТС (специальных технических средств)”.*

В постановлении **регламентируются деятельность**, связанная с использованием СТС, предназначенных для негласного получения информации. Лицензированию подлежат следующие виды деятельности:

– разработка и производство СТС;

– реализация СТС;

– приобретение СТС в целях продажи, ввоза и вывоза из РФ.

**Виды деятельности**, подлежащие лицензированию в области СТС (Постановление Правительства РФ от 12 апреля 2012 г. N 287 *"Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации"*):

* для негласного получения и регистрации акустической информации;
* для негласного визуального наблюдения и документирования;
* для негласного прослушивания телефонных переговоров;
* для негласного перехвата и регистрации информации с технических каналов связи;
* для негласного контроля почтовых отправлений;
* для негласного исследования предметов и документов;
* для негласного проникновения и обследования помещений, транспортных средств и других объектов;
* для негласного контроля за перемещением транспортных средств и других объектов;
* для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи;
* для негласной идентификации личности.

1. **Основные элементы системы обеспечения информационной безопасности РФ. Правовая база лицензирования и сертификации в РФ.**

Для **обеспечения ИБ РФ** действуют:

– совокупность органов (ФСБ, ФСТЭК, СБ), сил и средств, осуществляющих деятельность в области защиты информации (ЗИ);

– система лицензирования деятельности в области ЗИ;

– система сертификации средств ЗИ;

– система подготовки и переподготовки специалистов в области ЗИ.

**Лицензирование** – это процесс передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ. Получить право или разрешение на определенную деятельность может не каждый субъект, а только отвечающий определенным критериям в соответствии с правилами лицензирования. **Лицензия** – документ, дающий право на осуществление указанного вида деятельности в течение определенного времени.

**Сертификация** – это подтверждение соответствия продукции или услуг установленным требованиям или стандартам. **Сертификат** – документ, подтверждающий соответствие средства ЗИ требованиям по безопасности информации.

Законодательной и нормативной базой лицензирования и сертификации в области ЗИ **являются:**

**Законы РФ:**

– “О государственной тайне”;

– “О техническом регулировании”

– “О лицензировании отдельных видов деятельности;

– “О защите прав потребителей”;

**Постановления Правительства РФ:**

– “О лицензировании отдельных видов деятельности”

– “О лицензировании деятельности предприятий...”;

– “О сертификации средств ЗИ”.

А также Указы Президента РФ, и ряд других подзаконных актов.

1. **Виды деятельности в области защиты информации, подлежащие лицензированию. Порядок лицензирования, срок действия лицензии.**

**Лицензирование** – это процесс передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ. Получить право или разрешение на определенную деятельность может не каждый субъект, а только отвечающий определенным критериям в соответствии с правилами лицензирования. **Лицензия** – документ, дающий право на осуществление указанного вида деятельности в течение определенного времени.

Перечень видов деятельности в области ЗИ, на которые выдаются лицензии, определен Постановлением Правительства РФ - “О лицензировании отдельных видов деятельности” от 24.12.94 №1418 к ним, в частности, **относится разработка, производство, реализация и сервисное обслуживание**: шифровальных средств; защищенных систем телекоммуникаций; программных средств; специальных технических средств ЗИ; подготовка и переподготовка кадров.

Лицензированию подлежат следующие виды деятельности в области ЗИ:

* разработка, производство, распространение, техническое обслуживание и предоставление услуг в области шифрования информации; шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
* деятельность по выдаче сертификатов ключей ЭЦП, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;
* деятельность по выявлению электронных устройств негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
* деятельность по технической защите конфиденциальной информации;
* разработка, производство, реализация и приобретение в целях продажи СТС, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

**Схема последовательности действий**:

1. Прием лицензирующим органом заявления о предоставлении (продлении срока действия, переоформлении документа, подтверждающего наличие) лицензии
2. Проверка лицензирующим органом полноты и достоверности сведений о соискателе лицензии и возможности выполнения соискателем лицензии лицензионных требований и условий
3. Принятие лицензирующим органом решения о предоставлении или об отказе в предоставлении лицензии
4. Уведомление лицензирующим органом соискателя лицензии о предоставлении или об отказе в выдаче лицензии
5. Выдача лицензирующим органом соискателю лицензии документа, подтверждающего наличие лицензии (в случае принятия решения о предоставлении лицензии)
6. Занесение сведений о лицензиате в реестр лицензий.

Срок действия лицензии **не может быть** менее чем пять лет, если иное не предусмотрено настоящим Федеральным законом. Срок действия лицензии по его окончании может быть продлен по заявлению лицензиата.

1. **Организации, при которых созданы системы сертификации в РФ. Порядок и проведения сертификации средств защиты информации. В каких случаях сертификация носит добровольный характер?**

**Сертификация** – это подтверждение соответствия продукции или услуг установленным требованиям или стандартам. **Сертификат** – документ, подтверждающий соответствие средства ЗИ требованиям по безопасности информации.

Сертификация средств защиты конфиденциальной информации проводится в соответствии с Положением "О сертификации средств защиты информации", утвержденным ПП РФ от 23.04.96 N 509.

**Национальный орган по сертификации** определяется Правительством РФ. В настоящее время эти функции выполняет Федеральное агентство по техническому регулированию и метрологии (ФАТРиМ). Утверждены “Правила по проведению сертификации в РФ”, в соответствии с которыми целями сертификации являются:

* создание условий для деятельности предприятий и предпринимателей на товарном рынке РФ и участия в международной торговле;
* содействие потребителям в компетентном выборе продукции;
* содействие экспорту и повышение конкурентоспособности продукции;
* защита потребителя от недобросовестности изготовителя (продавца, исполнителя);
* контроль безопасности продукции для окружающей среды, жизни и имущества;
* подтверждение показателей качества продукции, заявленных изготовителями.

Организация сертификации средств ЗИ возлагается на ФСТЭК, ФСБ и МО в соответствии с функциями, возложенными на них законодательством РФ.

**Обязательной сертификации** (в соответствии с этим Положением) подлежат средства, в том числе иностранного производства, предназначенные для защиты информации, составляющей ГТ, и другой информации с ограниченным доступом, а также средства, использующиеся в управлении экологически опасными объектами.

В остальных случаях сертификация носит **добровольный характер** (добровольная сертификация) и осуществляется по инициативе разработчика, изготовителя или потребителя средства защиты информации.

**Принципы сертификации:**

* Сертификация изделий, обеспечивающих защиту ГТ является обязательной.
* Обязательность использования криптографических алгоритмов, являющихся стандартами.
* Принятие на сертификацию изделий только от заявителей, имеющих лицензию. В соответствии с вышеназванными документами, государственным организациям и предприятиям запрещено использование в информационных системах шифровальных средств, не имеющих сертификата.
* Кроме этого, в области информационных технологий действуют системы добровольной сертификации банковских технологий (МЕКАС) и средств связи.

**Порядок сертификации:**

* В Центральный орган по сертификации подается заявление и полный комплект технической документации.
* Центральный орган назначает испытательный центр (лабораторию) для проведения испытания.
* Испытания проводятся на основании хозяйственного договора между заявителем и испытательным центром.
* Сертификация (экспертиза материалов и подготовка документов для выдачи) осуществляется Центральным органом.

Сертификат **выдается** на срок до 5 лет.

1. **Правовая основа системы лицензирования и сертификации в области защиты конфиденциальной информации. Порядок лицензирования деятельности по технической защите и производству средств защиты конфиденциальной информации.**

**Срок действия лицензии** не может быть менее чем пять лет и может быть продлен по заявлению лицензиата. Продление срока действия лицензии осуществляется в порядке переоформления документа, подтверждающего наличие лицензии. ПП РФ от 15.08.2006 г. № 504 утвердило «Положение о лицензировании деятельности по технической защите конфиденциальной информации». Положение **определяет порядок лицензирования** данной деятельности, осуществляемой юридическими лицами и индивидуальными предпринимателями. Под технической защитой конфиденциальной информации понимается комплекс мероприятий по ее защите от несанкционированного доступа в целях ее уничтожения, искажения или блокирования доступа к ней.

**Лицензионные требования:**

* наличие в штате соискателя лицензии специалистов, имеющих высшее профессиональное образование в области технической защиты информации;
* наличие у соискателя лицензии помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации;
* наличие производственного, испытательного и контрольно-измерительного оборудования, прошедшего метрологическую поверку (калибровку), маркирование и сертификацию;
* использование АС, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших сертификацию;
* использование программ для ЭВМ и баз данных на основании договора с их правообладателем;
* наличие нормативных правовых актов, и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным ФСТЭК

**Схема последовательности действий:**

1. Прием лицензирующим органом заявления о предоставлении (продлении срока действия, переоформлении документа, подтверждающего наличие) лицензии
2. Проверка лицензирующим органом полноты и достоверности сведений о соискателе лицензии и возможности выполнения соискателем лицензии лицензионных требований и условий
3. Принятие лицензирующим органом решения о предоставлении или об отказе в предоставлении лицензии
4. Уведомление лицензирующим органом соискателя лицензии о предоставлении или об отказе в выдаче лицензии
5. Выдача лицензирующим органом соискателю лицензии документа, подтверждающего наличие лицензии (в случае принятия решения о предоставлении лицензии)
6. Занесение сведений о лицензиате в реестр лицензий
7. **Правовые основы деятельности органов, занимающихся оперативно-розыскной деятельностью. Виды ОРМ и условия проведение ОРМ, ограничивающих конституционные права человека.**

Деятельность этих органов основывается на Законе РФ “Об оперативно-розыскной деятельности”, от 12.08.95г. №144-Ф3 (ред. от 22.08.2004 №122-ФЗ). **Оперативно-розыскная деятельность** (ОРД) – вид деятельности, осуществляемый, гласно и негласно оперативными подразделениями уполномоченных государственных органов, в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств.

**Правовую основу оперативно-розыскной деятельности** составляют Конституция Российской Федерации, настоящий Федеральный закон, другие федеральные законы и принятые в соответствии с ними иные нормативные правовые акты федеральных органов государственной власти.

Оперативно-розыскными мероприятиями предусматривается проведение **следующих мероприятий:** Опрос; Наведение справок; Сбор образцов для сравнительного исследования; Проверочная закупка; Исследование предметов и документов; Наблюдение; Отождествление личности; Обследование помещений, зданий, сооружений, участков местности и транспортных средств; Контроль почтовых отправлений, телеграфных и иных сообщений; Прослушивание телефонных переговоров; Снятие информации с технических каналов связи; Оперативное внедрение; Контролируемая поставка; Оперативный эксперимент.

Проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека, допускается на основании судебного решения и **при наличии информации**:

1. О признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно.
2. О лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно.
3. О событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации.

**Основания** для проведения ОРМ:

* Наличие возбужденного уголовного дела.
* Ставшие известными органам, осуществляющим ОРД, **сведения о:** подготавливаемых, совершаемых или совершенных противоправных действиях, лицах их совершающих, если нет достаточных данных для возбуждения уголовного дела; лицах, скрывающихся от уголовного наказания; безвестном отсутствии граждан и обнаружении неопознанных трупов; событиях или действиях, создающих угрозу безопасности РФ.
* Поручения следователя, указания прокурора или определения суда по уголовным делам, находящимся в их производстве.
* Запросы других органов, осуществляющих оперативно-розыскную деятельность, по основаниям, указанным в настоящей статье.
* Постановление о применении мер безопасности в отношении защищаемых лиц.
* Запросы международных правоохранительных организаций и правоохранительных органов иностранных государств в соответствии с международными договорами РФ.

**Право осуществлять оперативно-розыскную деятельность** на территории РФ предоставлено:

* Органам внутренних дел РФ;
* ФСБ;
* Федеральным органам государственной охраны: Главному управлению охраны РФ и Службе безопасности Президента РФ;
* Таможенным органам РФ.
* Службе внешней разведки РФ.
* Федеральной службы исполнения наказаний.
* Органам по контролю за оборотом наркотических средств и психотропных веществ.

1. **Правовое регулирование деятельность ФСБ и полиции по соблюдению прав и свобод граждан. Условия беспрепятственного доступа сотрудниками правоохранительных органов в помещения и к информации юридических и физических лиц.**

Отдельным законом регулируется **деятельность ФСБ** – закон “Об органах ФСБ в РФ” от 3.04.95г. №40-ФЗ. В ст. 6 закона говорится о соблюдении прав и свобод человека при деятельности органов ФСБ. Полученные в процессе деятельности органов ФСБ сведения о частной жизни **не могут сообщаться** органами ФСБ без добровольного согласия гражданина. В случае нарушения сотрудниками органов ФСБ прав и свобод человека и гражданина руководитель ФСБ, прокурор или судья **обязаны принять** меры по восстановлению этих прав и свобод, возмещению причиненного ущерба и привлечению виновных к ответственности, предусмотренной законодательством. Должностные лица ФСБ, допустившие злоупотребление властью или превышение служебных полномочий, **несут ответственность**, предусмотренную законодательством РФ.

**Контроль за деятельностью органов ФСБ** осуществляют Президент, Федеральное Собрание и Правительство РФ (ст. 23). Надзор за исполнением органами ФСБ законов РФ осуществляют Генеральный прокурор РФ и уполномоченные им прокуроры (ст. 24).

**Вопросы**, связанные с полномочиями органов МВД отражены в Закон РФ «О полиции» от 7 февраля 2011 г. («О милиции» от 18 апреля 1991 г.) Законом определено, что сотрудники полиция **вправе** беспрепятственно входить в помещения, занимаемые предприятиями, учреждениями, организациями, независимо от подчиненности и форм собственности, только при наличии данных о влекущем уголовную или административную ответственность нарушении законодательства, и производить осмотр в присутствии не менее двух понятых и представителя юридического лица.

**Контроль за деятельностью полиции**, осуществляют Президент, Федеральное Собрание, Правительство РФ и органы законодательной и исполнительной власти субъектов РФ. Надзор за законностью деятельности полиции осуществляют Генеральный прокурор РФ и подчиненные ему прокуроры. Вред, причиненный гражданам, предприятиям, учреждениям и организациям сотрудником полиции, подлежит возмещению в порядке, предусмотренном гражданским законодательством.

1. **Законодательная база, регулирующая отношения по защите коммерческой информации от неправомерных действий контролирующих органов: ФАС, СЗС, банков.**

**Законодательной базой**, регулирующей правовые отношения с контролирующими и правоохранительными органами, являются следующие документы:

* Закон РФ “О защите конкуренции”
* Закон РФ “О конкуренции и ограничении монополистической деятельности на товарных рынках”
* Закон РФ “О полиции”, №3 ФЗ от 07 февраля 2011 г.
* Закон РФ “О санитарно-эпидемиологическом благополучии населения”
* Закон РФ “О банках и банковской деятельности”

Одной из форм недобросовестной конкуренции является, согласно закону “О защите конкуренции”, получение, использование, разглашение научно-технической, производственной или торговой информации, в том числе КТ без согласия ее законного владельца. К числу контролирующих органов **относится** федеральный антимонопольный орган, который имеет свои территориальные управления.

В настоящее время **функции федерального антимонопольного органа** осуществляет Федеральная антимонопольная служба (ФАС). Положение о Федеральной антимонопольной службе принято Правительством России 29 июля 2004 г.

Антимонопольный орган располагает для выполнения возложенных функций значительными полномочиями (беспрепятственный доступ в органы управления, на предприятия, право на ознакомление со всеми необходимыми документами и др.). Одна из его обязанностей – соблюдение КТ. Сведения о ней, полученные в порядке выполнения возложенных обязанностей, не подлежат разглашению.

В случае **разглашения сотрудниками** ФАС сведений, составляющих КТ, причиненные убытки подлежат возмещению в соответствии с гражданским законодательством. Информация, составляющая коммерческую, служебную, иную охраняемую законом тайну, представляется в антимонопольный орган в соответствии с требованиями, установленными федеральными законами и не подлежит разглашению, за исключением случаев, установленных федеральными законами.

За **разглашение информации**, составляющей коммерческую, служебную, иную охраняемую законом тайну, работники антимонопольного органа несут гражданско-правовую, административную и уголовную ответственность.

1. **Правовая защита объектов интеллектуальной собственности в соответствии с Гражданским кодексом часть 4. Формы правовой защиты объектов ИС.**

**Интеллектуальная собственность** (ГК часть 1, ст.138) – исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполненных работ или услуг (фирменное наименование, товарный знак и т.п.).

Существует три общепризнанные в мире правовые формы **защиты интеллектуальной собственности**: авторское право, патентное право и секреты производства - «ноу-хау».

Режим исключительных прав определен: Гражданским кодексом РФ, часть 4, от 18.12.2006г. № 230.

**Авторское право** – форма правовой защиты в отношении литературных, художественных и научных произведений.

**Патентное право** – форма правовой защиты в отношении изобретений во всех областях человеческой деятельности.

**Секреты производства (ноу-хау)** – форма правовой защиты любых полезных сведения (производственных, технических, экономических, организационных и других).

В РФ до недавнего времени действовали следующие законодательные акты, защищающие права граждан и юридических лиц на ОИС.

1. **Правовая защита коммерческой информации от неправомерных действий контролирующих и правоохранительных органов (законы РФ «О конкуренции», «О полиции»).**

**Правовая защита:**

* “О конкуренции и ограничении монополистической деятельности”
* “О защите конкуренции”

Законом **запрещается** как недобросовестная конкуренция:

* распространение ложных, неточных или искаженных сведений, которые могут причинить убытки хозяйствующему субъекту либо нанести ущерб его деловой репутации;
* введение в заблуждение в отношении характера, способа и места производства, потребительских свойств, качества и количества товара или в отношении его производителей;
* некорректное сравнение хозяйствующим субъектом производимых или реализуемых им товаров с товарами, производимыми или реализуемыми другими хозяйствующими субъектами;
* продажа, обмен или иное введение в оборот товара, если при этом незаконно использовались результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, средства индивидуализации продукции, работ, услуг;
* незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну.

**Вопросы**, связанные с полномочиями органов МВД отражены в Законе РФ «О полиции» от 7 февраля 2011 г. («О милиции» от 18 апреля 1991 г.).

**Законом** определено, что сотрудники полиция **вправе беспрепятственно** входить в помещения, занимаемые предприятиями, учреждениями, организациями, независимо от подчиненности и форм собственности, только при наличии данных о влекущем уголовную или административную ответственность нарушении законодательства, и производить осмотр в присутствии не менее двух понятых и представителя юридического лица.

**Контроль за деятельностью полиции**, осуществляют Президент, Федеральное Собрание, Правительство РФ и органы законодательной и исполнительной власти субъектов РФ. **Вред**, причиненный гражданам, предприятиям, учреждениям и организациям сотрудником полиции, **подлежит возмещению** в порядке, предусмотренном гражданским законодательством.

1. **Правовое регулирование информации в сети Интернет.**

В ст. 12 закона **«Об информации…»** говорится о необходимости создания условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет", но при этом делаются следующие ограничения.

**При использовании информационно-телекоммуникационных сетей передача информации осуществляется без ограничений при условии соблюдения требований к распространению информации и охране объектов интеллектуальной собственности.**

В законе “Об информации...” установлены нормы защиты прав пользователя информационными сетями:

Отправитель информации обязан обеспечить получателю возможность отказа от получаемой информации. Федеральными законами может быть предусмотрена обязательная идентификация лиц, использующих информационно-телекоммуникационную сеть. При этом получатель электронного сообщения вправе установить отправителя электронного сообщения.

**Единая система идентификации и аутентификации** – федеральная государственная информационная система, которая обеспечивает в случаях, предусмотренных законодательством РФ, санкционированный доступ к информации, содержащейся в информационных системах.

**Законодательная база:**

* **Статья 15.2.** Порядок ограничения доступа к информации, распространяемой с нарушением прав на фильмы.
* **Статья 10.1.** Обязанности организатора распространения информации в сети "Интернет".
* **Статья 13.31.** Неисполнение обязанностей организатором распространения информации в сети "Интернет ".

1. **Правовая защита профессиональной и служебной тайны в РФ. Виды профессиональной и служебной тайн.**

В современном законодательстве РФ **не принят закон** «О профессиональной тайне» и нет чёткого определения профессиональной тайны.

**Профессиональная тайна –**защищаемая по закону информация, доверенная лицу в силу исполнения им своих профессиональных обязанностей, не связанных с государственной и муниципальной службой и не являющаяся государственной или коммерческой тайной, распространение которой может нанести ущерб интересам лица, доверившего эти сведения.

**Виды профессиональной тайны**: Врачебная тайна. Тайна связи. Нотариальная тайна. Адвокатская тайна. Тайна усыновления. Тайна страхования. Тайна исповеди. Журналистская тайна.

**Правовые документы о профессиональной тайне:**

1. Законы РФ: «О СМИ», Семейный кодекс РФ, «О связи», «О религиозных объединениях», «Основы законодательства РФ о нотариате» и т.д.
2. Подзаконные акты: Постановления Правительства РФ: «Об утверждении правил оказания услуг телефонной связи»; «Об утверждении правил оказания услуг почтовой связи; «Об утверждении правил обязательного медицинского освидетельствования на выявление ВИЧ-инфекции» и др.
3. Судебная практика: постановление Конституционного суда РФ (в части профессиональной тайны адвоката); постановление Верховного суда РФ «Некоторые вопросы применения законодательства о компенсации морального вреда» и д.р.
4. **Правовое регулирование персональной тайны. основные положения закона РФ «О персональной тайне». Классификация информационных систем ПД.**

Отношения, связанные с обработкой персональных данных, осуществляемой органами государственной власти, юридическими и физическими лицами **регулируются** Законом РФ “О персональных данных”.

В законе дается различие общедоступных и конфиденциальных **персональных данных:**

* конфиденциальность персональных данных – обязательное требование не допускать их распространение без согласия субъекта персональных данных или законного основания;
* общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или в соответствии с федеральными законами.

Закон “О персональных данных” распространяется на всех участников (госучреждения, юридические и физические лица).

Законом регулируются отношения, связанные с обработкой ПД (сбор, систематизация, хранение, использование, распространение и т.п.) при использовании средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с ПД с использованием средств автоматизации.

В законе предусмотрены только четыре исключения, действие закона **не распространяется** на отношения, возникающие*: при обработке персональных данных для личных и семейных нужд; при обработке персональных данных в документах Архивного фонда РФ; при обработке персональных данных для включения их в Единый государственный реестр индивидуальных предпринимателей (ЕГРИП); при обработке персональных данных, отнесенных к государственной тайне.*

**Персональными данными гражданина**, подлежащим защите, признается любая информация, относящаяся к физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Безопасность ПД** достигается путем исключения несанкционированного, в том числе случайного, доступа к ним, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПД, а также иных несанкционированных действий.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

При обработке персональных данных в информационной системе **должно быть обеспечено**:

* предотвращение НСД к данным или передачи их лицам, не имеющим права доступа;
* своевременное обнаружение фактов НСД;
* недопущение воздействия средства обработки данных, в результате которого они могут быть, может быть нарушено их функционирование;
* возможность незамедлительного восстановления данных, измененных или уничтоженных при НСД;
* постоянный контроль за обеспечением уровня защищенности ПД.

По результатам анализа исходных данных типовой информационной системе присваивается **один из следующих классов:**

* класс 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов ПД;
* класс 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к негативным последствиям для субъектов ПД;
* класс 3 (К3) – информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПД;
* класс 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПД.

1. **Правовые основы защиты информации ограниченного доступа. Формирование перечня сведений, составляющих коммерческую тайну.**

В законе «Об информации…» нет термина «конфиденциальная информация», но дается определение понятия «конфиденциальность информации».

Указом Президента Российской Федерации был утвержден Перечень сведений «**конфиденциального характера**», где указаны **шесть видов такой информации**: персональные данные; тайна следствия и судопроизводства; служебная тайна; профессиональная тайна; коммерческая тайна; сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации о них.

**Отсутствие в законах четких определений видов информации** с ограниченным доступом (за исключением государственной тайны) приводит к противоречиям между данным указом и существующими законодательными актами, что затрудняет их исполнение.

Для обозначения грифа конфиденциальности используются следующие термины:

* **ОТ** – открытая информация;
* **ДВИ** – для внутреннего использования;
* **КИ** – конфиденциальная информация.

**Режим ограниченного доступа** включает режим государственной тайны (закон «О гос. тайне)» и режим конфиденциальности (***Указ Президента РФ №*** и регулируется законами: ***“О коммерческой тайне”, “О персональных данных”, “О вязи”, “О банках и банковской деятельности”, “О милиции” и др.)***.

**Информация составляет служебную или коммерческую тайну в случае**, когда информация (научно-техническая, технологическая, производственная, финансово-экономическая информация в том числе составляющая секреты производства (ноу-хау)) 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.

К коммерческой тайне относят следующие три группы сведений:

1. **Деловая информация** (о сферах деятельности): данные о себестоимости продукции и услуг; деловые планы и планы производства и развития; соглашения, предложения, контракты и т.п.
2. **Техническая информация:** научно-исследовательские проекты; конструкторская документация на продукцию; дизайн, передовые технологии и оборудование; химические формулы и т.п.
3. **Информация о клиентах и конкурентах**. На каждого клиента фирмы накапливается информация, где отражаются его привычки, о представляемых ему фирмой привилегиях и т.п. Аналогичные базы данных составляют и на своих конкурентов. Таким образом, формируются «профиль клиента» и «профиль конкурента».

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.

***Закон "О коммерческой тайне"*** регулирует отношения, связанные с отнесением информации к КТ, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестнойконкуренции, а также определяет сведения, которые не могут составлять КТ.

1. **Актуальность защиты коммерческой информации, угрозы и методы защиты, правовая защита.**

В условиях жесткой конкуренции фирмы сбор информации о рынке, о партнерах и другой полезной информации как правило носит разведывательный характер. Главным предметом разведки является **коммерческая тайна**.

Понятие “коммерческая тайна” отражено в **Законе РФ "О коммерческой тайне".** К коммерческой тайне относят следующие три группы сведений:

1. **Деловая информация** (о сферах деятельности): данные о себестоимости продукции и услуг; деловые планы и планы производства и развития; соглашения, предложения, контракты и т.п.
2. **Техническая информация:** научно-исследовательские проекты; конструкторская документация на продукцию; дизайн, передовые технологии и оборудование; химические формулы и т.п.
3. **Информация о клиентах и конкурентах**. На каждого клиента фирмы накапливается информация, где отражаются его привычки, о представляемых ему фирмой привилегиях и т.п. Аналогичные базы данных составляют и на своих конкурентов. Таким образом, формируются «профиль клиента» и «профиль конкурента».

Существует **три основных направления сбора информации,** представляющей коммерческий интерес.

* Информация о рынке (издается и публикуется).
* Информация о производстве продукции (закупки, наблюдение, опрос).
* Информация об организационных особенностях и планах развития.

Сведения о деятельности фирмы и ее руководителях собирают в различных экономических газетах и журналах, справочниках, выписывают у биржевиков, покупают у частных детективов, а также с помощью конкурентной разведки через Интернет. **Принято различать:** конкурентную разведку ("деловая разведка", "бизнес-разведка") и промышленный шпионаж. **Отличие** заключается в соблюдении закона в первом случае и нарушениях уголовного, авторского или любого другого права – во втором.

**Конкурентная разведка** – это сбор и обработка информации законными способами.

На данный момент в нашей стране под конкурентной разведкой подразумеваются четыре вида сбора информации:

1. Сбор данных о партнерах и клиентах для предотвращения мошенничеств с их стороны.
2. Информация о потенциальных партнерах и сотрудниках. Обычно этим занимаются отделы безопасности компаний или частные детективные агентства
3. Выполнение услуг охраны и сыска, предусмотренных Законом "О частной детективной и охранной деятельности ".
4. Сбор информации маркетингового характера.

**Виды конкурентной разведки**: наблюдение; отчеты торговых работников, поиск информации в открытых БД, анализ годовых отчетов предприятий.

**Промышленный шпионаж –** незаконный сбор сведений, составляющих коммерческую тайну.

Для обозначения степени важности коммерческой информации для предприятия можно предложить систему обозначения степени ее секретности:

1. Коммерческая тайна – строго конфиденциально (КТ-СК)
2. Коммерческая тайна – конфиденциально (КТ-К)
3. Коммерческая тайна (КТ)

Рекомендуется использовать промежуточный гриф ДВИ (для внутреннего использования).

**Доступ работника** к информации, составляющей КТ, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями. Органы государственной власти, несут гражданско-правовую ответственность за разглашение или незаконное использование КТ их должностными лицами, которым она стала известна в связи с выполнением ими должностных обязанностей.

Лицо, которое использовало информацию, составляющую КТ, и не имело достаточных оснований считать использование данной информации незаконным, (получило доступ к ней в результате случайности или ошибки), **не может быть привлечено к ответственности**.

**Ответственность за разглашение КТ, дана в *УК РФ ст. 183* –** Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну:

1. Собирание сведений, составляющих коммерческую тайну, незаконным способом – наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы либо лишением свободы на срок до двух лет.
2. Незаконные разглашение или использование сведений, составляющих коммерческую, наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы либо лишением свободы на срок до 3-х лет.
3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, наказываются штрафом в размере до двухсот тысяч рублей или либо лишением свободы на срок до пяти лет.
4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие **тяжкие последствия**, наказываются лишением свободы на срок **до десяти лет**.

**МОДУЛЬ 2: УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ 2023 (КНЯЗЕВА М.В.)**

1. **Системный подход к управлению ИБ. Политики безопасности. Определение, сферы приложения, верхний, средний, нижний уровни политик безопасности. Законодательный уровень. Административный уровень. Процедурный уровень. Технический уровень.**

**Законодательный уровень**: Обзор нормативно-правовых актов РФ в области информационной безопасности

**Административный уровень**: Разработка политик информационной безопасности (организационно-технические и режимные меры).

**Политика информационной безопасности** — набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области ЗИ. На основе ПИБ строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение ИС в различных ситуациях.

Для конкретной ИС политика безопасности должна быть индивидуальной. Она зависит от технологии обработки информации, используемых программных и технических средств, структуры организации и т.д.

**Процедурный уровень**: перечень основных организационно-технические мероприятия по защите информации.

**Технический уровень**: конкретные меры и их реализация.

**Верхний уровень**: документация на уровне руководства (управление ресурсами безопасности и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими организациями, обеспечивающими или контролирующими режим безопасности).

**Средний уровень**: частные политики безопасности, политики использования средств криптозащиты, политики антивирусной защиты, политики мониторинга и управления инцидентами и т. п. (определяет решение вопросов, касающихся отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых организацией. Примеры таких вопросов — отношение к доступу в Internet, использование домашних компьютеров и т. д.)

**Нижний уровень**: действия по обеспечению ИБ на уровне сетевых сервисов, руководства, инструкции, регламенты, правила администрирования (исходит из соображений целостности, доступности и конфиденциальности. В общем случае цели должны связывать между собой объекты сервиса и осмысленные действия с ними.).

1. **Защита критической информационной инфраструктуры России (КИИ). ГосСОПКА.**

*Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 367.*

Под **критической информационной инфраструктурой** РФ (КИИ) подразумевается совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов РФ и обеспечивающих их взаимодействие информационно- телекоммуникационных сетей, а также ИТ-систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка.

**ГосСОПКА** – это государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Согласно указу Президента РФ от 22.12.2017 No620, ГосСОПКА предназначена для выполнения **четырех основных задач**: прогнозирование в области информационной безопасности РФ; взаимодействие организаций-владельцев информационных ресурсов, в том числе – субъектов критической информационной инфраструктуры, в ходе работ по обнаружению, предупреждению и ликвидации последствий кибератак; контроль степени защищенности информационных ресурсов РФ от кибератак; расследование компьютерных инцидентов.

**Ответственность за функционирование системы** ГосСОПКА лежит на Федеральной службе безопасности РФ.

**ФЗ-187 от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации».**

* Статья 7. Категорирование объектов критической информационной инфраструктуры: три категории значимости. Критерии значимости: Социальная значимость (5 показателей); Политическая значимость (2 показателя); Экономическая значимость (3 показателя); Экологическая значимость (1 показатель); Значимость для обеспечения обороны страны, безопасности государства и правопорядка (3 показателя).
* Статья 8. Реестр значимых объектов критической информационной инфраструктуры.
* Статья 10. Система безопасности значимого объекта критической информационной инфраструктуры.

**Этапы реализации требований приказа ФСТЭК РФ No239:**

1. Первичный сбор данных. На начальном этапе организация определяет, является ли она субъектом КИИ. Для этого она готовит перечни ИС, АСУ, ИТС и определяет сферы функционирования каждой из них. **Результат этой работ**ы — вывод о необходимости (или отсутствии необходимости) выполнения организацией требований 187-ФЗ.

2. Проведение категорирования. Организация создает комиссию по категорированию, определяет объекты категорирования, а затем определяет категории значимости для объектов КИИ. После этого она согласует со ФСТЭК России перечень объектов КИИ с присвоенными (либо не присвоенными) категориями значимости.

3.1. Для субъектов КИИ, **не имеющих** значимые объекты КИИ. В том числе это относится к организациям, у которых нет значимых объектов КИИ, так как организация должна обеспечить соответствие 9 статьи ФЗ-187 (часть 2), в частности незамедлительно информировать о компьютерных инцидентах федеральные органы исполнительной власти.

3.2. Для субъектов КИИ, **имеющих** значимые объекты КИИ. Разработать план реагирования на компьютерные инциденты.

**Требования приказа ФСТЭК РФ No239**

29.3. Прикладное программное обеспечение, планируемое к внедрению в рамках создания значимого объекта и обеспечивающее выполнение его функций по назначению должно соответствовать следующим требованиям по безопасности:

29.3.1. **Требования по безопасной разработке программного обеспечения:**

* наличие руководства по безопасной разработке программного обеспечения;
* проведение анализа угроз безопасности информации программного обеспечения;
* наличие описания структуры программного обеспечения на уровне подсистем и результатов сопоставления функций программного обеспечения и интерфейсов

29.3.2. **Требования к испытаниям по выявлению уязвимостей в программном обеспечении:**

* проведение статического анализа исходного кода программы;
* проведение фаззинг-тестирования программы, направленного на выявление в ней уязвимостей;
* проведение динамического анализа кода программы (для программного обеспечения, планируемого к применению в значимых объектах 1 категории значимости).

29.3.3. **Требования к поддержке безопасности программного обеспечения:**

* наличие процедур отслеживания и исправления обнаруженных ошибок и уязвимостей программного обеспечения;
* определение способов и сроков доведения разработчиком (производителем) программного обеспечения до его пользователей информации об уязвимостях программного обеспечения, о компенсирующих мерах по защите информации или ограничениях по применению программного обеспечения, способов получения пользователями программного обеспечения его обновлений, проверки их целостности и подлинности;
* наличие процедур информирования субъекта критической информационной инфраструктуры об окончании производства и (или) поддержки программного обеспечения (для программного обеспечения, планируемого к применению в значимых объектах 1 категории значимости).

1. **Управление информационной безопасностью. Построение СОИБ и СУИБ на предприятии.**

**Система обеспечения информационной безопасности** —технические и организационные меры, механизмы с помощью которых можно активно реагировать на инциденты информационной безопасности и обеспечивать общий уровень защищенности.

**Целью** проектирования системы обеспечения информационной безопасности (СОИБ) является выработка рекомендаций, организационных и технических решений по обеспечению безопасности информационных ресурсов хранимых, обрабатываемых и передаваемых по каналам связи в компьютерных сетях и информационных системах организации.

В состав СОИБ обычно входят следующие **компоненты и подсистемы**, тесно интегрированные между собой и с другими компонентами **ИТ-инфраструктуры**: подсистема защиты периметра сети; подсистема обеспечения безопасности межсетевых взаимодействий; подсистема мониторинга и аудита безопасности; подсистема обнаружения и предотвращения атак; подсистема резервного копирования и восстановления данных; подсистема анализа защищенности и управления политикой безопасности; подсистема контроля целостности данных и другие.

**Основные функции СУИБ**:

1. Выявление и анализ рисков информационной безопасности

2. Планирование и практическая реализация процессов, направленных на минимизацию рисков ИБ

3. Контролирование этих процессов

4. Внесение в процессы минимизации информационных рисков необходимых корректировок.

Условно АСУИБ можно разделить на **три функциональных уровня**:   
уровень сбора —> уровень ядра —> уровень управления. (по возрастанию).

**Уровень ядра.** Здесь происходит сбор, анализ и обнаружение корреляции между событиями безопасности, поступающими от систем обеспечения информационной безопасности и различных компонент ИТ-инфраструктуры. Обычно уровень ядра строится на основе одной из представленных на рынке SIEM-систем (Security Information and Event Management).

*SIEM-система — это программный или программно-аппаратный комплекс, его основной функцией является обработка большого количества событий безопасности, порождаемых различными системами, и генерация на их основе инцидентов информационной безопасности. От миллионов сообщений и log- записей осуществляется переход к небольшому количеству настоящих инцидентов ИБ.*

Уровень ядра предназначен для сбора, анализа и корреляции событий безопасности, поступающих от систем безопасности и выполняет следующие **функции**:

* сбор событий от систем обеспечения информационной, физической и экономической безопасности, ИТ-систем;
* анализ событий в соответствии с предустановленными правилами корреляции для генерации инцидентов;
* анализ событий в соответствии с пользовательскими правилами корреляции для генерации инцидентов;
* автоматическая генерация инцидентов при срабатывании одного из соответствующих правил корреляции, которая может основываться как на отдельном событии, так и на агрегации и сопоставлении разнородных событий и сетевых потоков;
* возможность автоматической инвентаризации сетевых узлов.
* и другие…

**Уровень сбора** предназначен для сбора, нормализации и отправки на уровень ядра событий безопасности, поступающих от антивирусных приложений, систем защиты от несанкционированного доступа, различных систем мониторинга и обнаружения вторжений, систем межсетевого экранирования, защиты почты, DLP, сетевого оборудования, серверов и т. д.

**Уровень управления –** это набор организационных мер, организационно-распорядительной документации и те средства визуализации и отчетности, которые предоставляет SIEM-система. **Функции** **управления** информационной безопасностью: визуализация данных и создание отчетов о состоянии ИБ на предприятии, управление и хранение истории инцидентов ИБ, ведение реестров информационных активов, поддержание в актуальном состоянии документации в области управления ИБ и т.д.

Основные **задачи автоматизации**, выполняемые Уровнем управления, в зависимости от комплектации, это:

* **Управление информационными активами организации:** поддержание в актуальном состоянии информации о бизнес-процессах, информационных системах, технических сервисах, ПО и информации и т.д.
* **Управление жизненным циклом инцидентов** ИБ в организации: оповещение о возникновении инцидентов информационной безопасности и т.д.
* **Управление записями/логами информационной безопасности**. Структурированное хранение и индексация лог- записей от различных систем, поиск данных и расследование инцидентов ИБ, сбор и хранение улик в соответствии с законодательством УК РФ;
* **Управление соответствием требованиям информационной безопасности организации:** законодательным требованиям;заданным ключевым показателям эффективности;внутренним и отраслевым стандартам организации;международным стандартам.
* **Управление рисками информационной безопасности организации за счет автоматизации:** подготовки модели угроз и модели нарушителя;подготовки перечня информационных активов и объектов среды;определения источников угроз для каждого из типов объектов среды;проведения оценки возможности реализации угроз информационной безопасности и тяжести последствий и т.д.
* **Управление знаниями.** Помощь в принятии решений по управлению ИБ организации, в том числе по возникающим инцидентам информационной безопасности **за счет:** автоматически регулярно пополняемой базы знаний и рекомендаций и т.д.

1. **Угрозы информационной безопасности.**

Использование DFD диаграмм для построения модели угроз информационной безопасности. Microsoft Threat Modeling Tool. Примеры.

<https://learn.microsoft.com/ru-ru/azure/security/develop/threat-modeling-tool>

**Угроза** — представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

**Источником угрозы** могут быть: злоумышленники, обслуживающий персонал, техногенные аварии, стихийные бедствия.

**Уязвимость** – это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации

**Критичность реализации угрозы** – степень влияния реализации угрозы на ресурс, т. е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах. Состоит из критичности реализации угрозы по конфиденциальности, целостности и доступности

**Модель угроз** – описание существующих угроз ИБ, их актуальности, возможности реализации и последствий.

Стандартная **модель** безопасности информации **«CIA»:** **конфиденциальность** (confidentiality) – сохранение информации в тайне, невозможность раскрытия информации без согласия заинтересованных сторон; **целостность** (integrity) – непротиворечивость и правильность информации, защита информации от неавторизованной модификации; **доступность** (availability) - обеспечение наличия информации и работоспособности основных услуг для пользователя в нужное для него время.

**Модель угроз «Гексада Паркера»** Parkerian Hexad вводит еще три состояния: **подлинность** (authenticity) – в применении к пользователю соответствие участника взаимодействия своему имени; **управляемость, или владение** (possession or control ) – гарантия того, что законный владелец является единственным лицом, во власти которого изменить информацию или получить к ней доступ на чтение; **полезность** (utility) – удобство доступа; нахождение информации в такой форме, что ее владелец не должен тратить неоправданных усилий.

**Модель безопасности информации «5A»: Authentication** (аутентификация: кто ты?), **Authorization** (авторизация: что тебе можно делать?)**, Availability** (доступность: можно ли получить работать с данными?)**, Authenticity** (подлинность: не повреждены ли данные злоумышленником?)**, Admissibility** (допустимость: являются ли данные достоверными, актуальными и полезными?)

**DFD** — общепринятое сокращение от англ. data flow diagrams — диаграммы потоков данных. Так называется методология графического структурного анализа, описывающая внешние по отношению к системе, источники и адресаты данных, логические функции, потоки данных и хранилища данных, к которым осуществляется доступ.

**Диаграмма потоков данных** (data flow diagram, DFD) — один из основных инструментов структурного анализа и проектирования информационных систем, существовавших до широкого распространения UML.

STRIDE — это аббревиатура от названий угроз нарушения каждого из перечисленных **состояний ИС**: **spoofing**, аутентичности; **tampering**, целостности; **repudiation**, апеллируемости; **information disclosure**, конфиденциальности; **denial of service**, доступности; **elevation of privilege**, авторизованности.

**Модель актуальных угроз ИС:** диаграммы потоков данных (DFD)

**Элементы верхнеуровневой DFD для моделируемой системы**.

* процесс — компонент ИС, осуществляющий обработку или передачу информации;
* интерактор — внешний, по отношению к ИС компонент, осуществляющий информационный обмен с каким-либо компонентом ИС;
* хранилище — компонент ИС, осуществляющий хранение или передачу информации;
* поток данных — канал обмена информацией между процессами, интеракторами и хранилищами;
* граница доверия — проходит через потоки данных и отделяет доверенные компоненты ИС от недоверенных.

На основании актуальности угроз для каждого из типов компонентов **оценивается**: угрозы для процессов; S и R для интеракторов; T,R,I,D для хранилищ; T,I,D для потоков данных.

На основании информации о пересечении потоками данных границ доверия строится список актуальных угроз для модели. Далее производится декомпозиция каждого из элементов диаграммы так, как если бы этот компонент был отдельной ИС, причем потоки данных, циркулирующие внутри него, также размечаются границами доверия, если это необходимо. По полученной DFD вновь строится список актуальных угроз, дополняющий предыдущий. Этот процесс повторяется рекурсивно до тех пор, пока достигнутая степень детализации модели не перестанет вносить новые актуальные угрозы, либо пока возможна декомпозиция.

1. **Стандарт OWASP (Open Web Application Security Project). Рейтинг OWASP Top 10 2021 десяти наиболее опасных рисков информационной безопасности для веб-приложений и мобильных рисков.**

**Open Web Application Security Project (OWASP)** – это некоммерческая организация, а также открытое интернет-сообщество, целью которого является защита организаций посредством разработки безопасного кода, тестирования на проникновение и сопровождения разрабатываемых приложений на всех этапах проекта.

OWASP использует различные ресурсы (люди, технологии, процессы), чтобы решить существующие и возникающие проблемы в разработке безопасных приложений.

Это происходит с помощью внедрения библиотек и применения инструментов безопасности, предоставляемых OWASP.

<https://owasp.org/Top10/>

Open Web Application Security Project 2021 представляет собой **нумерованный список угроз**:

A1: Неверное управление доступом

А2: Криптографические ошибки и сбои

А3: Инъекция

А4: Небезопасный дизайн

А5: Неверная конфигурация безопасности

А6: Использование уязвимых и устаревших компонент

А7: Ошибки идентификации и аутентификации

А8: Ошибки целостности программного обеспечения и данных

А9: Ошибки логирования и мониторинга безопасности

А10: Подделка запросов на стороне сервера

A1: Неверное управление доступом (Broken Access Control). **Пример**.

**Управление доступом** применяет политику таким образом, что пользователи не могут действовать за пределами своих предполагаемых разрешений. Сбои обычно приводят к несанкционированному раскрытию информации, модификации или уничтожению всех данных или к выполнению бизнес-функции за пределами полномочий пользователя.

**Нарушения** предполагают:

* Обход проверок управления доступом путем изменения URL-адреса (изменение параметров или принудительный просмотр), внутреннего состояния приложения или HTML-страницы либо с помощью инструмента атаки, изменяющего запросы API.
* Разрешение просмотра или редактирования чужой учетной записи путем предоставления ее уникального идентификатора (небезопасные прямые ссылки на объекты).
* Доступ к API с отсутствующими элементами управления доступом для POST, PUT и DELETE.
* Манипуляции с метаданными, такие как воспроизведение или подделка маркера управления доступом JSON Web Token (JWT), а также использование файла cookie или скрытого поля для повышения привилегий или злоупотребления аннулированием JWT.
* Неправильная конфигурация CORS разрешает доступ к API из неавторизованных/ненадежных источников.
* Принудительный просмотр аутентифицированных страниц в качестве неаутентифицированного пользователя или привилегированных страниц в качестве обычного пользователя.

**Критерии оценки рисков:** распространенность соответствующих уязвимостей в приложениях (Weakness Prevalence), сложности их обнаружения (Weakness Detectability) и эксплуатации (Exploitability), а также критичности последствий их эксплуатации (Technical Impacts).

**Примеры сценариев атаки**

Сценарий No 1. Приложение использует непроверенные данные в вызове SQL, который обращается к информации об учетной записи:

pstmt.setString(1, request.getParameter("acct"));

ResultSet results = pstmt.executeQuery( );

Злоумышленник просто изменяет параметр «acct» браузера, чтобы отправить любой номер учетной записи, который он хочет. В случае неправильной проверки злоумышленник может получить доступ к учетной записи любого пользователя.

https://example.com/app/accountInfo?acct=notmyacct

Сценарий No 2. Злоумышленник просто заставляет просматривать целевые URL-адреса. Для доступа к странице администратора требуются права администратора.

https://example.com/app/getappInfo

https://example.com/app/admin\_getappInfo

Если неавторизованный пользователь может получить доступ к любой странице, это недостаток.

1. Протокол автоматизации управления данными безопасности (SCAP).

**SCAP** (Security Content Automation Protocol) — спецификация, которая определяет три процесса: поиск и исправление уязвимостей, автоматическую настройку конфигураций, а также оценку уровня безопасности.

Например, SCAP состоит из следующих **стандартов**:

* Типовые уязвимости и ошибки конфигурации (Common Vulnerabilities and Exposures CVE(r))
* Список типовых конфигураций (Common Configuration Enumeration CCETM)
* Список типовых платформ (Common Platform Enumeration CPE)
* Единая система определения величины риска уязвимостей (Common Vulnerability Scoring System CVSS)
* Расширяемый формат описания списка проверки конфигурации (Extensible Configuration Checklist Description Format XCCDF) https://scap.nist.gov/specifications/xccdf/
* Открытый язык описания уязвимостей и оценки (Open Vulnerability and Assessment Language OVALTM)
* Перечень общеизвестных слабых мест (Common Weakness Enumeration, CWE);
* Система оценки общеизвестных слабых мест (Common Weakness Scoring System, CWSS);

**Протокол автоматизации управления данными безопасности** (SCAP) представляет собой набор открытых стандартов, определяющих технические спецификации для представления и обмена данными по безопасности. Эти данные могут быть использованы для автоматизации процесса поиска уязвимостей, оценки соответствия технических механизмов контроля и измерения уровня защищенности.

SCAP (Security Content Automation Protocol) включает в себя ряд открытых стандартов, поддерживаемых международным сообществом профессионалов в области информационной безопасности. Последняя версия SCAP состоит из одиннадцати компонентов протокола в пяти категориях.

<https://csrc.nist.gov/projects/security-content-automation-protocol/>

**Компоненты SCAP** (The Security Content Automation Protocol).

1. **Языки.** Языки SCAP стандартизуют словари и выражения, описывающие политику безопасности, механизмы контроля и результаты оценки. SCAP включает в себя **следующие компоненты:**

* Расширяемый формат описания контрольного списка конфигураций (XCCDF, Extensible configuration checklist description format);
* Открытый язык описания уязвимостей и проведения оценок (OVAL, Open vulnerability and assessment language);
* Открытый интерактивный язык описания контрольного списка (OCIL, Open checklist interactive language).

2. **Формат отчетов**. Форматы отчета SCAP представляют необходимые конструкции, для выражения собранной информации в стандартизированных форматах:

* Формат представления данных об активах ИБ (Asset Reporting Format);
* Формат для уникальной идентификации активов ИБ на основе идентификаторов (Asset Identification [AI]).

3. **Перечни.** Перечни SCAP определяют стандартизованные спецификации, официальные перечни (словари), выраженные с использованием этих спецификаций. SCAP включает в себя следующие перечни:

* Общий перечень платформ (CPE , Common platform enumeration);
* Общий перечень конфигураций (CCE , Common configuration enumeration);
* Общий перечень уязвимостей и рисков (CVE, Common vulnerabilities and exposures).

4. **Измерение и оценка систем.** В SCAP это выражается в оценке определенных особенностей уязвимости (например, слабых мест программного обеспечения и проблем конфигурации безопасности) и определении количественного значения влияния уязвимости (метрики). Метрики SCAP в терминах системных технических требований описываются:

* Общей системой оценки уязвимости (CVSS, Common vulnerability scoring system)
* Общей системой оценки конфигурации (CCSS, Common configuration scoring system).

5. **Целостность**. Спецификация целостности SCAP предназначена для обеспечения целостности информационного SCAP-контента и полученных с помощью него результатов. Модель доверия для данных об автоматизации безопасности (TMSAD, Trust Model for Security Automation Data) является спецификацией целостности SCAP.

1. **Управление рисками информационной безопасности. Основные положения согласно международному стандарту ISO/IEC 27 005: Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.**

**Управление рисками информационной безопасности** по своей сути является ядром системы менеджмента информационной безопасности (СМИБ) [ГОСТ Р ИСО/МЭК 27001 Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности - Требования].

В общем случае процесс включает в себя следующие **этапы**:

1. Установление контекста: определение области оценки рисков ИБ, установление внешних и внутренних факторов.
2. Оценка рисков ИБ, включающая в себя: идентификацию риска ИБ; анализ риска ИБ; сравнительную оценку риска ИБ; оценку остаточного риска (при необходимости).
3. Обработка рисков ИБ (снижение, перенос, уклонение, принятие).
4. Мониторинг и пересмотр рисков ИБ.
5. Документирование и отчетность.

**Внешний контекст** (external context): внешняя среда, в которой организация стремится к достижению своих целей.

**Внутренний контекст** (internal context): внутренняя среда, в которой организация стремится к достижению своих целей.

**Вероятность реализации** – это вероятность того, что конкретная уязвимость будет проэксплуатирована и приведет к пагубным влияниям в бизнес-процессах. Например, уязвимость может и существовать, но условия работы системы не будут позволять ее проэксплуатировать.

**Документ «Положение о применимости»** – документированное предписание, определяющее цели и меры управления, соответствующие и применимые к системе менеджмента информационной безопасности организации.

**Обработка информационных рисков** (принятие, уклонение, передача, снижение). Варианты обработки риска должны выбираться исходя из результатов оценки риска, предполагаемой стоимости реализации этих вариантов и их ожидаемой эффективности. Должны реализовываться такие варианты, при которых значительное снижение риска может быть достигнуто при относительно небольших затратах. Четыре варианта обработки риска не являются взаимоисключающими. В отдельных случаях организация может получить значительную выгоду от объединения вариантов, таких, как снижение вероятности риска, уменьшение последствий и перенос или сохранение любого остаточного риска

**Составляющими процесса управления рисками** являются процедурысвоевременного выявления рисков (risk identification), их оценка (risk assessment) и последующая обработка (risk treatment).

**Методология оценки рисков** информационной безопасности предусматривает такие шаги:

* выявление уязвимостей (организационных и технических);
* выявление угроз, направленных на рассматриваемые активы; • определение последствий от реализации угроз;
* выявление существующих контролей (контрмер);
* определение вероятности реализации угроз.

**Активы** существуют **основные и вспомогательные**

**Основные:** бизнес-процессы и информация

**Вспомогательные:** аппаратные средства, носители информации, программное обеспечение, бизнес-приложение, персонал, место функционирования организации, организация.

**Определение ценности активов.**

В соответствии с их критичностью с точки зрения важности активов для осуществления бизнес–целей организации. Затем ценность активов определяется с использованием двух мер:

– восстановительной стоимости актива – стоимости его очистки с целью восстановления и замены информации (если это возможно);

– последствий для бизнеса от потери или компрометации актива, например, возможные неблагоприятные последствия для бизнеса и/или законодательные или регулирующие последствия раскрытия, модификации, недоступности и/или разрушения информации, а также других информационных активов.

(Ценность активов, от которых зависят другие активы, может изменяться следующим образом:

– если ценность зависимых активов (например, данных) ниже или равна ценности рассматриваемого актива (например, программного обеспечения), его ценность остается такой же;

– если ценность зависимых активов (например, данных) выше ценности рассматриваемого актива (например, программного обеспечения), его ценность должна быть увеличена в соответствии со степенью зависимости или ценностью других активов.)

**Оценка влияния инцидентов на активы.**

Различные угрозы и уязвимости могут иметь различное влияние на активы, например, потеря конфиденциальности, целостности и доступности. Поэтому оценка последствий связана с определением ценности активов или становится связанной, исходя из анализа влияния на бизнес. Также нужно учитывать, что ценность актива определяется не только его внутренними свойствами и качествами но еще и тем с какими другими активами он связан и как они подвержены инцидентам.

1. **Управление рисками информационной безопасности. Составляющие процесса управления рисками: процедуры своевременного выявления рисков (risk identification), их оценка (risk assessment) и последующая обработка (risk treatment).**

**Суть работы** по **управлению рисками** состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры по уменьшению этого размера и затем убедиться, что риски заключены в приемлемые рамки. **Управление рисками** включает в себя два вида деятельности, которые чередуются **циклически**: (пере)оценку (измерение) рисков; выбор эффективных и экономичных защитных средств (нейтрализация рисков).

**Risk identification**. **Целью** идентификации риска является процесс выявления, исследования и описания рисков. Идентификация включает идентификацию источников риска, событий, их причин и возможных последствий. Идентификация риска может включать статистические данные, теоретический анализ, обоснованную точку зрения и заключение специалиста, а также потребности заинтересованной стороны.

**Risk assessment** — это количественное определение затрат, связанных с видами риска, которые были выявлены на первом этапе управления риском. Оценка риска позволяет оценить вероятность того, что неблагоприятное событие может негативно повлиять на бизнес, экономику, проект или инвестиции.

**Risk treatment** — это процесс изменения риска. Обработка риска **может включать**: избегание риска посредством принятия решения не начинать или не продолжать деятельность, в результате которой возникает риск; принятие риска или увеличение риска для достижения цели; устранение источника риска; изменение возможности возникновения; изменение последствий; разделение риска с другой стороной или сторонами; принятие риска на основании обоснованного решения.

**VaR** — это величина убытков, которая с вероятностью уровня доверительного интервала (к примеру, 99%), не будет превышена. Достоинства оценки с помощью VaR: рассчитать риски для всех возможных рынков; рассчитать риск потерь в соответствии с вероятностью их появления

**VaR = k \* σ \* Y**, где k – коэффициент, определенного доверительного интервала, Y – стоимостной объем актива, σ – волатильность курса валюты. Для каждого доверительного интервала существует свой коэффициент (множитель k).

**Однократный ущерб на ресурс** определяется по формуле: **SLE = AV \* EF**, где AV — ценность ресурса, в которую входят все виды затрат на него (установка, сопровождение и т.п.), EF — доля этой величины, утрачиваемая в результате вредоносного действия. Так как не все угрозы равновероятны, вводят годичную частоту реализации угрозы (ARO). Тогда **ожидаемый годовой ущерб** от данной угрозы будет вычисляться по формуле: **ALE = SLE \* ARO**. Оценка значения ARO может производиться на основе анализа статистики нарушений информационной безопасности.

1. **Управление рисками информационной безопасности. Идентификация и оценка технических уязвимостей. Расчет рисков по методике CVSS 3.0 Common Vulnerability Score System. Общая система оценки уязвимостей.**

**Общая система оценки уязвимостей CVSS** (Common Vulnerability Scoring System) – открытая схема для обмена и оценки уязвимостей. В этой системе используется группа метрик, а также дается описание базовых метрик [base metrics], вектора уязвимости [vector] и оценок уязвимости. Каждая метрика представляет собой число (оценку) в интервале от 0 до 10. **Группа метрик CVSS 3.0:**

**Базовая метрика:** используется для описания основополагающих сведений об уязвимости - возможности эксплуатации уязвимости и воздействии уязвимости на систему, не изменяются со временем и не зависят от среды.

**Временные метрики** [temporal] метрики учитывается время, например опасность уязвимости снижается с выходом официального обновления.

**Контекстные метрики** [environmental] вопросы контекста, среды принимаются во внимание при оценке опасности уязвимости. Например, чем больше системы подвержены уязвимости, тем выше её опасность.

Компоненты системы, для которых рассчитываются метрики: **Уязвимый компонент** (vulnerable component) – компонент, содержащий уязвимость, которую можно эксплуатировать. **Атакуемый компонент** (impacted component) – те, конфиденциальность, целостность и доступность которого могут пострадать при успешной реализации атаки.

В большинстве случаев уязвимый и атакуемый компоненты совпадают, но есть **исключения**: выход за пределы песочницы приложения; получение доступа к пользовательским данным, сохранённым в браузере, через уязвимость в веб-приложении.

**Базовая метрика** отображает основные **характеристики** уязвимости: Вектор атаки (AV), Сложность атаки (AC), Требуемые привилегии (PR), Взаимодействие с пользователем (пользовательский интерфейс), Область (S), Влияние на конфиденциальность (C), Влияние целостности (I), Влияние доступности (A). AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**Формулы расчета риска:**

**R = P(t) \* S**, где R – значение риска; P(t) – вероятность реализации угрозы ИБ; S – степень влияния угрозы на актив.

**R = P(t) \* P(v) \* S**, где R – значение риска; P(t) – вероятность реализации угрозы ИБ; P(v) – вероятность наличия уязвимости; S – ценность актива.

**R = S \* L(t) \* L(v)**, где R – значение риска; S – ценность актива/ресурса; L(t) – уровень угрозы; L(v) – уровень/степень уязвимости.

1. **Управление рисками информационной безопасности. База Common Weakness Enumeration. Классификация общеизвестных слабых мест CWE.**

**CWE** (Common Weakness Enumeration) – общий перечень уязвимостей и недостатков безопасности программного обеспечения. **Цель** CWE состоит в том, чтобы обеспечить более эффективное обсуждение, описание, отбор и использование инструментальных средств и услуг по защите программного обеспечения, которые могут обнаруживать эти слабые места в кодах источников и операционных системах, а также улучшить понимание слабых мест программного обеспечения, связанных с его архитектурой и проектированием, и управление этими слабыми местами.

**Данные об уязвимостях** формируются из национальной базы данных уязвимостей США (U.D. National Vulnerability Database (NVD)). Оценка уязвимости формируется из частоты (**частота упоминаний**), с которой какой-либо недостаток (CWE) является основной причиной уязвимости, и потенциальной **опасности эксплуатации.** В конце вычисляется итоговая оценка путём перемножения оценки частоты упоминания на оценку серьёзности.

1. **Управление рисками информационной безопасности. Common Weakness Scoring System – CWSS - Общая система оценки «слабых мест».**

**Общая система оценки слабых мест** (CWSS) предоставляет механизм для определения приоритетов слабых мест программного обеспечения последовательным, гибким и открытым способом. CWSS разделен на три группы показателей: **Base Finding** (базовый результат поиска), **Attack Surface** (область атаки) и **Environment** (среда).

Группа показателей **Base Finding**: охватывает внутренние риски, присущие слабому месту, доверие к точности результатов поиска, а также действенность средств контроля. В нее **входят:** Техническое воздействие, приобретенная привилегия уровень приобретенной привилегии, эффективность внутреннего контроля, доверие к результатам поиска.

Группа показателей **Attack Surface**: барьеры, которые должен преодолеть злоумышленник, для того чтобы эксплуатировать слабое место. В нее **входят:** Требуемая привилегия, Уровень требуемой привилегии, Вектор доступа, Сложность аутентификации, Уровень взаимодействия, Масштаб развертывания.

Группа показателей **Environment**: характеристики слабого места, присущие конкретной среде или операционному контексту. В нее **входят:** Воздействие на деятельность, Вероятность обнаружения, Вероятность эксплуатации, Эффективность внешнего контроля, Распространенность.

Каждому параметру в группе показателей базовых результатов поиска присваивается значение. Эти значения преобразуются в соответствующие им весовые коэффициенты и рассчитывается элемент оценки базовых результатов поиска, который может находиться в интервале от 0 до 100. Аналогичный метод применяется к группам показателей области атаки и среды; их элементы оценки могут находиться в интервале от 0 до 1. Наконец, эти три элемента перемножаются, и в результате получается оценка CWSS в интервале от 0 до 100.

1. **CWE/SANS Top 25 Most Dangerous Software Errors. Наиболее Опасные Ошибки ПО. Примеры. Классификация общеизвестных слабых мест CWE.**

**Топ 25 ошибок ПО:**

CWE-787 – Запись вне границ

CWE-79 – Неправильная нейтрализация входных данных при создании веб-страницы ("Межсайтовый скриптинг")

CWE-89 – Неправильная нейтрализация специальных элементов, используемых в команде SQL ("SQL-инъекция")

CWE-20 – Неправильная проверка входных данных

CWE-125 – Чтение вне границ

CWE-78 – Неправильная нейтрализация специальных элементов, используемых в команде операционной системы ("Внедрение команды операционной системы")

CWE-416 – Используйте после Бесплатного

CWE-22 – Неправильное ограничение имени пути к каталогу с ограниченным доступом ('Обход пути')

CWE-352 – Подделка межсайтовых запросов (CSRF)

CWE-434 – Неограниченная загрузка файла с опасным типом

CWE-476 – Разыменование нулевого указателя

CWE-502 – Десериализация ненадежных данных

CWE-190 – Переполнение целого числа или обтекание

CWE-287 – Неправильная аутентификация

CWE-798 – Использование жестко закодированных учетных данных

CWE-862 – Отсутствует авторизация

CWE-77 – Неправильная нейтрализация специальных элементов, используемых в команде ("Командная инъекция")

CWE-306 – Отсутствует аутентификация для критической функции

CWE-119 – Неправильное ограничение операций в пределах буфера памяти

CWE-276 – Неправильные разрешения по умолчанию

CWE-918 – Подделка запросов на стороне сервера (SSRF)

CWE-362 – Параллельное выполнение с использованием общего ресурса с неправильной синхронизацией ("Условие гонки")

CWE-400 – Неконтролируемое потребление ресурсов

CWE-611 – Неправильное ограничение ссылки на внешнюю сущность XML

CWE-94 – Неправильный контроль генерации кода ("Внедрение кода")

**Данные об уязвимостях** формируются из национальной базы данных уязвимостей США (U.D. National Vulnerability Database (NVD)). Оценка уязвимости формируется из частоты (**частота упоминаний**), с которой какой-либо недостаток (CWE) является основной причиной уязвимости, и потенциальной **опасности эксплуатации.** В конце вычисляется итоговая оценка путём перемножения оценки частоты упоминания на оценку серьёзности.

1. **Управление инцидентами информационной безопасности.**

**SOC** (Security Operations Center) – комплекс, предназначенный для централизованного сбора и анализа информации о событиях, поступающих из различных источников автоматизированной системы компании. **Основные задачи**, которые должен решать SOC:

* Инвентаризация и контроль инфраструктуры (мониторинг ИТ-инфраструктуры, сбор данных об оборудовании и его характеристиках, контроль состава ИТ-систем, построение связей взаимодействия между компонентами и т.д.);
* Консолидация информации об инцидентах ИБ;
* Координация и автоматизация реагирования на инциденты ИБ;
* Интеграция и получение данных из внешних источников;
* Сбор показателей эффективности системы защиты (метрик).

**SIEM** (Security information and event management) - объединение двух терминов, обозначающих область применения ПО: **SIM** (Security information management) — управление информационной безопасностью, и **SEM** (Security event management) — управление событиями безопасности. **Задачи SIEM:**

* сбор, анализ и представление информации от сетевых устройств и устройств безопасности, приложений идентификации (управления учетными данными) и управления доступом;
* инструментов поддержания политики безопасности и отслеживания уязвимостей;
* операционных систем, баз данных и журналов приложений, а также сведений о внешних угрозах;
* управление привилегиями пользователей и служб, сервисам директорий и другим изменениям конфигурации,
* обеспечение аудита и обзора журналов, реакции на инциденты.

**Функционал SIEM:**

**Агрегация данных**: управление журналами данных; данные собираются из различных источников: сетевые устройства и сервисы, датчики систем безопасности, серверы, базы данных, приложения; обеспечивается консолидация данных с целью поиска критических событий.

**Корреляция**: поиск общих атрибутов, связывание событий в значимые кластеры. Технология обеспечивает применение различных технических приемов для интеграции данных из различных источников для превращения исходных данных в значащую информацию.

**Оповещение**: автоматизированный анализ коррелирующих событий и генерация оповещений о текущих проблемах. Оповещение может выводиться на «приборную» панель самого приложения, так и быть направлено в прочие сторонние каналы.

**Средства отображения**: отображение диаграмм помогающих идентифицировать паттерны отличные от стандартного поведения.

**Совместимость**: применение приложений для автоматизации сбора данных, формированию отчетности для адаптации агрегируемых данных к существующим процессам управления информационной безопасностью и аудита.

**Хранение данных**: применение долговременного хранилища данных в историческом порядке для корреляции данных по времени и для обеспечения трансформируемости. Долговременное хранение данных критично для проведения компьютерно-технических экспертиз, поскольку расследование сетевого инцидента вряд ли будет проводиться в сам момент нарушения.

**Экспертный анализ**: возможность поиска по множеству журналов на различных узлах; может выполняться в рамках программно-технической экспертизы

1. **Управление инцидентами информационной безопасности. Системы поведенческого анализа - User and Entity Behavioral Analytics (UBA).**

**Система поведенческого анализа** – User and Entity Behavioral Analytics (UBA) – класс систем, позволяющих на основе массивов данных о пользователях и ИТ-сущностях (конечных станциях, серверах, коммутаторах и т. д.) с помощью алгоритмов машинного обучения и статистического анализа строить модели поведения пользователей и определять отклонения от этих моделей, как в режиме реального времени.

В качестве **источников данных** для UBA-систем могут выступать: файлы журналов серверных и сетевых компонентов, журналы систем безопасности, локальные журналы с конечных станций, данные из систем аутентификации и содержание переписки в социальных сетях, мессенджерах и почтовых сообщениях.

**Основные задачи:**

**Прикладная аналитика** данных из различных источников, как простая статистическая, так и расширенная, с использованием методов машинного обучения, в режиме реального времени и/или с определенной периодичностью.

**Быстрая идентификация атак** и других нарушений, большинство из которых не определяются классическими средствами ИБ.

**Приоритизация событий**, консолидированных из разных источников (SIEM, DLP, AD и т. д.), для более оперативного реагирования со стороны администраторов ИБ.

Более **эффективная реакция на события** за счет предоставления администраторам ИБ расширенной информации об инциденте, включающей все объекты, которые были вовлечены в аномальную активность.

1. **Управление инцидентами информационной безопасности. APT (англ. advanced persistent threat — «развитая устойчивая угроза»; целевая кибератака).**

**APT** (англ. advanced persistent threat — «развитая устойчивая угроза»; также целевая кибератака) – противник, обладающий современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения (например, информационных, физических и обманных).

**Цель –** осуществление намерений извлечения информации, срыва или создания помех критическим аспектам выполняемой задачи, программы или службы; либо для того, чтобы занять позицию, позволяющую осуществить эти намерения в будущем.

**Типовой сценарий APT-атаки:**

1. Рассылки по электронной почте
2. Доставка вредоносного кода
3. Запуск Вредоносного кода
4. Закрепление в системе
5. Получение канала для скрытого управления
6. Повышение локальных привилегий
7. Локальный сбор и анализ информации
8. Сбор информации по сети
9. Распространение в смежные системы
10. Получение высоких привилегий в домене
11. Поиск и получение ценной информации
12. Скрытая выгрузка, утечка данных
13. Обеспечить возможность удаленного доступа в дальнейшем

**The Cyber Kill Chain** описывает стадии, которые проходит злоумышленник для успешной реализации своей деятельности:

**Разведка** – Исследование, идентификация и выбор свой жертвы, часто используя публичные источники данных - соцсети, сайты конференций, списки рассылки и т.п.

**Вооружение** – Оснащение вредоносным содержанием файла (например, PDF или MS Office) или иного контента, который должен быть прочтен/открыт жертвой.

**Доставка** – Донесение вредоносного контента до жертвы, чаще всего используя для этого e-mail, web-сайты или USB-флешки.

**Заражение** – Запуск вредоносного кода, используя имеющиеся на целевом компьютере уязвимости, с последующим его заражением.

**Инсталляция** – Открытие удаленного доступа для незаметного управления и обновления вредоносного кода. В последнее время для этого чаще всего используется протокол DNS.

**Получение управления** – Получение обновлений с новым функционалом извне, а также управляющих команд для достижения поставленных целей.

**Выполнение действий** – Сбор и кража данных, шифрование файлов, перехват управления, подмена данных и другие задачи, которые могут стоять перед нарушителем.

1. **Управление инцидентами информационной безопасности. IoC (Indicator of Compromise) - Показатели компрометации.**

**Индикаторы компрометации** – в компьютерной криминалистике предмет, наблюдаемый в сети или в операционной системе, который с высокой достоверностью указывает на вторжение в компьютер.

**Типичными IoC** являются сигнатуры вирусов и IP-адреса, хэши MD5 файлов вредоносных программ или URL-адреса или доменные имена серверов управления и контроля сервера. После выявления IOC в процессе реагирования на инциденты и компьютерной криминалистики их можно использовать для раннего обнаружения будущих попыток атак с использованием систем обнаружения вторжений и антивирусного программного обеспечения.

**Характерные признаки компрометации** – это имеющие определенное состояние свойства и измеряемые события безопасности, связанные с работой компьютеров и сетей.

**Индикаторы компрометации IoC (Computer Forensics)** – это конструкции, доказательства после инцидента, используемые для подачи характерных признаков компрометации в совокупности с контекстной информацией с целью представления артефактов и/или заслуживающего внимания поведения в контексте кибербезопасности, например, хэш MD5, C&C-домен, прописанный в коде IP-адрес, ключ реестра, имя файла и др. Они постоянно изменяются.

**Индикаторы атаки IoA** – это набор конструкций, состоящий из неизвестных атрибутов, индикаторов компрометации IoC, контентной и контекстной информации, анализируемой в режиме реального времени, динамически.

**Отличия:**

IoC:

* Фиксируют уже случившийся факт заражения
* Точечное обнаружение во времени. IoC устаревают.
* Представляют информацию о конкретной угрозе
* Просто детектировать

IoA:

* Обнаруживают неизвестные атаки, для которых еще нет индикаторов компрометации
* Постоянное обнаружение в режиме real-time
* Абстрагированы от конкретных наблюдаемых случаев в отдельных конкретных инцидентах
* Сложно детектировать

1. **Управление инцидентами информационной безопасности. STIX (Structured Threat Information eXpression).**

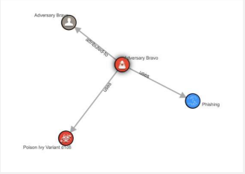
В условиях же появления совершенного нового класса угроз – APT (Advanced Persistent Threats), задача оперативного обмена информацией о них стала как никогда актуальной. **Идея STIX** достаточно проста – этот протокол должен устранить вышеназванный недостаток. Он позволяет унифицировать описание различных угроз и связанных с ними параметров – индикаторы атаки, информация об инциденте, используемый для атаки инструментарий или уязвимости, предполагаемые меры нейтрализации атаки, информация о предполагаемом противнике/нарушителе, а также о его тактике, используемой технике и процедурах, кампания, в рамках которой осуществляется атака (например, Red October) и т.п. Но STIX только стандартизует описание угроз, но не отвечает на вопрос, как обмениваться информацией о них? Эту задачу решает второй протокол, разработанный MITRE в паре со STIX – протокол TAXII, который и унифицирует способы обмена информации об угрозах, описанных с помощью STIX.

**STIX** (Structured Threat Information eXpression) – стандарт, используемый для предоставления унифицированной информации о киберугрозах (CTI).

Позволяет совместно использовать описание различных угроз и связанных с ними параметров в различных областях. STIX предоставляет унифицированную информацию об инцидентах, включая:

* информационные объекты (например, создание ключа реестра, сетевой трафик на определенные IPадреса, отправка email с определенного адреса и т.д.);
* индикаторы; инциденты;
* тактики, методы, процедуры атакуемого (шаблоны атак, вредоносные программы, эксплойты и т. д.);
* объекты эксплуатации (например, уязвимости, ошибки безопасности или неправильные конфигурации);
* способы противодействия (реагирование на инциденты или устранение уязвимостей/ошибок безопасности);
* группы кибер-атак (наборы инцидентов, TTP);
* участники киберугроз (идентификация, характеристики противника).

**Приведите пример в формате JSON:** Описаны связи между злоумышленником Adversary Bravo, используемой им техникой атаки -- фишингом - и вредоносным ПО Poison Ivy Variant d1c6.В этом случае при обнаружении в инфраструктуре вредоносного ПО Poisonlvy вариант d1c6 такая структура фида с взаимосвязями поможет понять, что подобным вредоносным ПО пользуется злоумышленник.



1. **Источники поступления информации об угрозах. Threat Intelligence: цели, задачи, этапы. Платформы Threat Intelligence.**

Платформы TI предназначены, в первую очередь, для сбора индикаторов компрометации из различных источников.

**Атака → Компрометация → Утечка данных → Обнаружение инцидента → Реагирование и Устранение**

При этом согласно ежегодному отчету по информационной безопасности Cisco специалисты по безопасности в течение своего рабочего дня способны обработать лишь 56% поступающих сообщений об угрозах, а среди этих оповещений об угрозах обоснованным признается только каждое второе (т.е. 28%). Таким образом, 44% инцидентов остаются без внимания!

**Задачи Threat Intelligence:**

* **Разведка и сбор данных об уязвимостях и угрозах.** TI должна быть интегрирована в систему защиты и должна предоставлять возможность централизованного сбора информации из открытых и закрытых источников об уязвимостях и угрозах.
* **Аналитика.** TI должна анализировать и накапливать базу знаний по обнаружению, раскрытию, разработке и выдаче рекомендаций по реагированию на угрозы.
* **Обмен данными.** TI также должна предоставлять возможность обмена полученными данными в режиме реального времени. Аналитическая информация должна мгновенно распространяться в стандартизированном формате как внутренним, так и внешним средствам защиты.
* **Оперативное оповещение.** TI должна оперативно оповещать об атаках и угрозах в любой конечной точке, используя единую стандартизированную базу с классифицированными данными.

**Этапы:**

* **Analysis** – анализ. На данном этапе проводится анализ угрозы по отношению к атаке (Threat Intelligence vs. Indicators, Threat models, Attack trees/graphs, the Cyber Kill Chain).
* **Assessment & Triage** – оценка уровня риска и приоретизация threat types and attack vectors.
* **Controls** – контроли безопасности и решения в области ИБ

1. **Анализ данных из открытых источников OSINT. Цели и задачи. OSINT в сфере информационной безопасности. Анализируемые данные.**

**OSINT** (Open Sourсe INtelligence) — разведывательная дисциплина и комплекс мероприятий, инструментов иметодов для получения и анализа информации из открытых источников. Он применяется в отношении конкретных людей, организаций, а также событий, явлений и целей.

В IT-индустрии и информационной безопасности OSINT помогает:

* собирать информацию о конкурентах и искать конкурентные преимущества;
* анализировать защищенность объекта, выявлять уязвимые точки системы безопасности;
* находить информационные утечки;
* выявлять возможные угрозы, их источники и направленность;
* анализировать киберпреступления (кражи данных, взломы и т.д.).

**ИСТОЧНИКИ ДАННЫХ ДЛЯ OSINT.** Open source intelligence подразумевает получение данных из источников в общественном достоянии и/или таких, доступ к которым возможен по запросу. К ним относятся:

* информационные материалы (статьи, новости, заметки) в СМИ; научные исследования, опубликованные в специализированных изданиях; книги, посты и комментарии в социальных сетях;
* форумы, блоги, сайты обмена видео, такие как YouTube.com, вики, Записи Whois о зарегистрированных доменных именах, метаданных и цифровых файлов, даркнет-ресурсы, данные геолокации, IP-адреса;
* информация из переписи;
* документы из открытых государственных и негосударственных архивов;
* публичные коммерческие данные (доход, прибыль, убыток, рост, стоимость акций и т.д.);
* результаты публичных опросов;
* данные со спутников дистанционного зондирования Земли и самолетов аэрофотосъемки;
* полицейские и судебные документы и другие источники.

**ПАССИВНЫЕ И АКТИВНЫЕ МЕТОДЫ. Пассивный** – позволяют получать общую информацию об объекте. Она собирается вручную или с помощью специальных сервисов и инструментов, упрощающих сбор, систематизацию и анализ данных. Например, программ для парсинга сайтов. К пассивным методам **можно отнести:**

* сбор информации (в том числе по фотографиям) из открытых поисковых систем;
* анализ пользовательской активности в социальных сетях и блогах, на форумах, иных виртуальных платформах;
* поиск открытых персональных данных пользователей в социальных сетях, мессенджерах;
* просмотр сохраненных копий сайтов в поисковых системах, интернет-архиве;
* получение геолокационных данных с помощью общедоступных ресурсов вроде Google Maps или Яндекс.Карты.

**Активные** – такие методы подразумевают непосредственное влияние аналитика на исследуемый объект, использование специализированных средств получения данных или совершение действий, требующих определенных усилий. К активным методам **можно отнести:**

* сбор данных на закрытых ресурсах, доступ к которым возможен только по подписке;
* применение специализированных сервисов и программ, которые активно воздействуют на исследуемый объект — например, автоматически регистрируются на сайте;
* использование сервисов, сканирующих приложения, файлы или сайты на наличие вредоносного кода;
* создание поддельных веб-ресурсов, каналов в мессенджерах, собирающих данные пользователей, конфиденциальные или секретные сведения.

В логике OSINT пассивные методы, направленные на сбор общей информации из легкодоступных источников, предваряют применение активных способов, предназначенных для сбора конкретных данных об объекте.

**АВТОМАТИЗИРОВАННЫЕ ИНСТРУМЕНТЫ.**

**Shodan** – это поисковая система, предназначенная для нахождения подключенных к интернету устройств по IPv4-адресам (роутеры, камеры видеонаблюдения, датчики безопасности и т.д.). Сама система не наносит вреда, но с ее помощью любой желающий при должном старании может найти незащищенное или плохо защищенное устройство.

**Metagoofil** – это метапоисковая система, которая использует другие поисковики для нахождения и извлечения находящихся в открытом доступе файлов PDF, Word, Powerpoint и Excel. С ее помощью можно парсить техническую документацию, клиентские базы данных, справочники, каталоги и прочие полезные источники.

**Maltego** – это графический анализ данных Инструмент OSINT предназначенный для поиска данных о людях, компаниях. Работает на платформах Windows, Linux и MacOS. Ключевая особенность программы в том, что она определяет соотношения между данными, создает графическое отображение данных. На графиках и диаграммах можно просматривать до 1млн объектов. Maltego автоматизирует поиск, что позволяет пользователям одним кликом выполнить несколько запросов.

**WHOIS** (от англ. who is — «кто это?») — сетевой протокол прикладного уровня, базирующийся на протоколе TCP (порт 43). Основное применение — получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем.

1. **Компьютерная криминалистика (Computer Forensics). Определение, цели и задачи. Специальные методы, применяемые для раскрытия и расследования компьютерных преступлений.**

**Компьютерная расследовании криминалистика** (Форензика) – прикладная наука о раскрытии и преступлений, связанных с компьютерной информацией, о методах получения и исследования доказательств, имеющих форму компьютерной информации (цифровых доказательств), о применяемых для этого технических средствах. **Основные задачи** компьютерной криминалистики:

1. Создание методов, аппаратных и программных инструментов для сбора и исследования доказательство компьютерных преступлений
2. Разработка тактики оперативно-розыскных мероприятий (ОРМ) и следственных действий, связанных с компьютерной информацией
3. Установление компьютерно криминалистических характеристик правонарушений: выявление факта правонарушения; установление причин и источников; определение методов; восстановление обстоятельств и хронологии событий; формирование доказательной базы и обеспечение ее целостности для правового преследования виновных лиц; выявление новых способов правонарушений

**Специальные методы:**

1. Создание и применение специализированных криминалистических информационных систем (пр. платформы киберразведки – threat intelligence)
2. Использование в целях обнаружения или исследования доказательств публичных поисковых систем (таких как Google ), а также специализированных (таких как Shodan, Censys – IoT и других)
3. Создание виртуальной личности для целей проведения с ее помощью ОРМ и агентурной работы
4. Сбор хеш функций известны файлов для отделения их от файлов, содержащих оригинальную пользовательскую или модифицированную информацию
5. Архивирование полного содержимого носителей для целей последующего расследования возможных инцидентов
6. Эмулирование сетевых и операционных сервисов для исследования поведения подозрительных действий и программ в лабораторных условиях (пр. honeypots - ловушки, sandboxing - песочницы)

**Этапы сбора цифровых доказательств:**

* Поиск цифровых носителей информации
* Сохранение целостности содержимого цифровых носителей информации
* Анализ содержимого цифровых носителей информации
* Изложение результатов по содержимому цифровых носителей информации

**Программные блокираторы записи:**

* функции для монтирования ФС в режиме «только чтение» в ОС Linux
* с использованием загрузочной операционной системы, которая не отправляет каких-либо команд записи, без функций автомонтирования (лайв ОС)

**Аппаратные криминалистические копировальщики с блокировкой записи:**

* автономные (Tableau forensic duplicator), судебный режим всегда включен (хеширование MD5 и SHA-1).
* встраиваемые в ЭВМ (Tableau forensic bridge.

1. **Компьютерная криминалистика (Computer Forensics). Волатильные данные и их сбор – Live Forensics. Какую информацию можно с помощью них найти и проанализировать?**

**Сбор доказательств:**

1. Произвести вскрытие коробки компьютера для внутреннего осмотра, а также обеспечения доступа к физическим интерфейсам устройств хранения данных.
2. Идентификация накопителей, с которых должны быть собраны доказательства.
3. Документация накопителей и аппаратной конфигурации системы: Характеристики накопителя; Внутренние компоненты системы
4. Отсоединить накопитель от кабеля питания для вероятного предотвращения изменений, повреждений или удаления данных на нем.
5. Произвести контролируемую загрузку для идентификации информации с BIOS и проверки его функциональности.
6. При возможности создание образов копии накопителей произвести на машине экзаменатора.
7. Должна быть инициирована Защита от записи! Экзаменатор перед тем как произвести непосредственный сбор доказательств должен также инициировать вычисление контрольных сумм (хеширование)
8. Логирование всех действий: Экзаменатор должен документировать детали действий при осуществлении сбора данных, включая фотографирования накопителей, описание используемого программно-аппаратного обеспечения, временные метки, уникальные идентификаторы накопителей, использованные директории, хеши, размеры данных
9. Логи могут быть созданы как на бумажном, так и на электронном носителе информации соблюдая юридические аспекты обеспечения целостности и неотказуемости.