Вопросы к экзамену

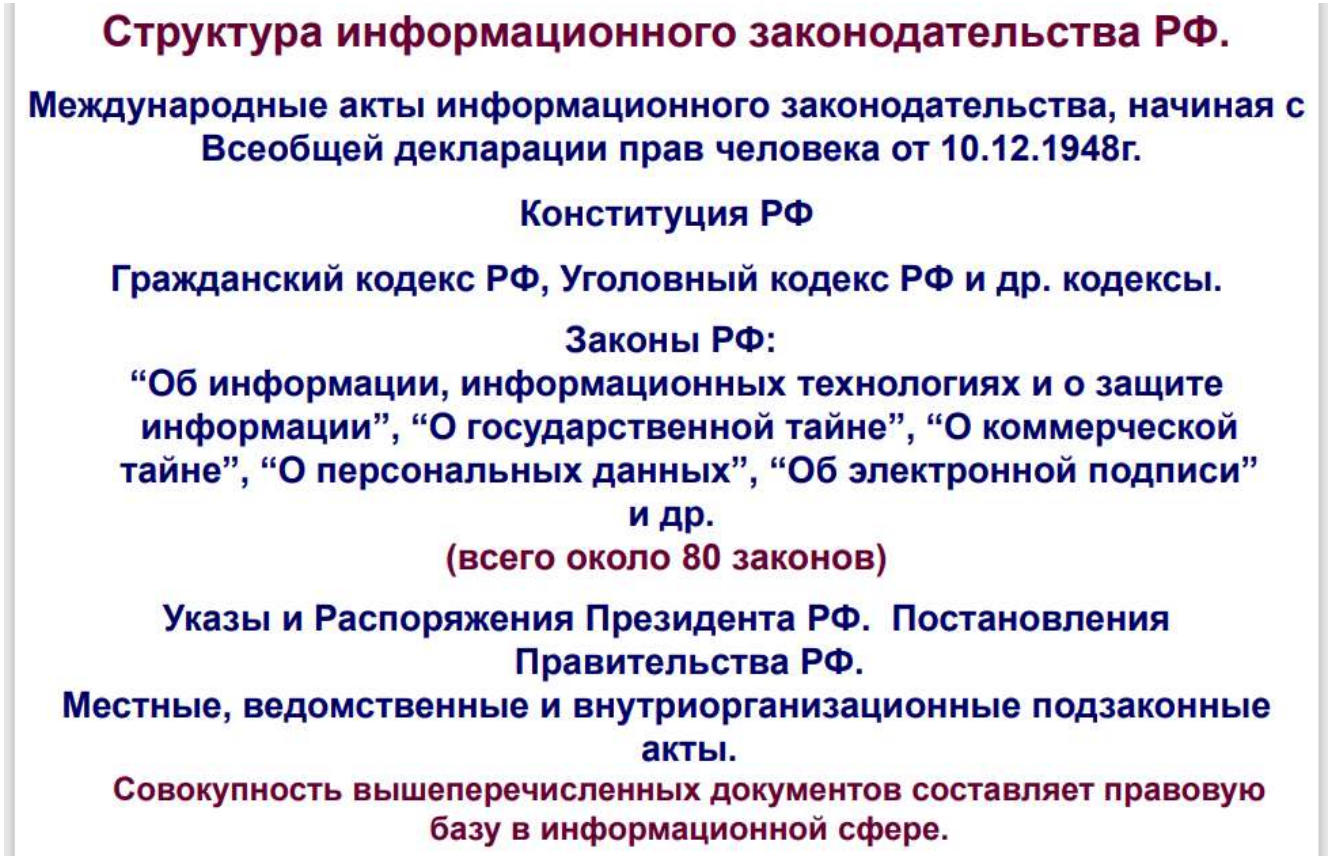
МОДУЛЬ 1: **ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (СТРУКОВ В.И.)**

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

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

В юриспруденции представлены много таких составляющих, которых объединяет одна общая научная дисциплина - теория государства и права. Она изучает закономерности возникновения, развития, назначения и функционирования государства и права.

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



Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти

Информационное законодательство имеет следующую структуру.

Международные акты информационного законодательства, начиная с Всеобщей декларации прав человека от 10.12.1948г.

Конституция РФ, Гражданский кодекс РФ, Уголовный кодекс РФ и др.

Закон 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 другие подзаконные акты.

2. Место информационного права в системе права. Свойства информационного товара.

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

Вертикальное строение права - это совокупность следующих элементов: Отрасль права, Институт права, Норма права

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

Регулятивные отрасли устанавливают права и обязанности участников правоотношений.

Информационное право регулирует комплекс общественных отношений, связанных с информацией, защитой информации, защитой прав собственников информационных ресурсов, формирования различных институтов тайн (государственной, служебной, банковской, коммерческой, личной и т.п.)

Информационный продукт сохраняет содержащуюся в нем информацию, независимо от того, сколько раз она была использована.

Информационный продукт со временем подвергается своеобразному «моральному износу» (информация может терять свою ценность по мере того, как предоставляемое ею знание перестает быть актуальным).

Разным потребителям информационных товаров и услуг удобны разные способы предоставления информации, ведь потребление информационного продукта требует усилий. В этом состоит свойство адресности информации.

Производство информации, в отличии от производства материальных товаров, требует значительных затрат по сравнению с затратами на тиражирование. В связи с этим при обмене на информационном рынке покупатель приобретает носитель, а не право копирования. Это свойство информационного продукта создает, в частности, немало проблем в связи с определением прав собственности в рамках сферы информационной деятельности.

информационное право занимает самостоятельное место в системе российского права в качестве комплексной отрасли, его нормы регулируют

специфические группы информационных отношений, составляющих обособленный, но тесно взаимосвязанный с иными отраслями права предмет

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

Под ***информационным преступлением*** следует понимать виновное общественно опасное деяние, запрещенное Уголовным кодексом РФ под угрозой наказания, совершенное в области информационных правоотношений.

Уголовная ответственность за информационные преступления определяется рядом статей Уголовного кодекса Российской Федерации, расположенных в различных разделах и главах:

- преступления против свободы, чести и достоинства личности (гл. 17) (клевета (ст. 129), оскорбление (ст. 130));
- преступления против конституционных прав и свобод человека и гражданина (гл. 19) (нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138), отказ в предоставлении гражданину информации (ст. 140), нарушения избирательных прав или работы избирательных комиссий (ст. 141), воспрепятствование законной профессиональной деятельности журналистов (ст. 144), нарушение авторских и смежных прав (ст. 146), нарушение изобретательских и патентных прав (ст. 147).)

Административным правонарушением признается противоправное, виновное действие (бездействие) физического или юридического лица, за которое КоАП РФ или законами субъектов Российской Федерации об административных правонарушениях установлена административная ответственность. КоАП РФ содержит информационные правонарушения в большинстве глав, описывающих составы административных правонарушений (главы 5 - 8, 10, 13 - 17, 19 и 21).

В главе 13 "Административные правонарушения в области связи и информации" предусмотрена ответственность:

- за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11) и правил защиты информации (ст. 13.12);
- за незаконную деятельность в области защиты информации (ст. 13.13);

Дисциплинарную ответственность за проступки в информационной сфере несут работники предприятий, учреждений, организаций в соответствии с положениями, уставами, правилами внутреннего трудового распорядка и другими нормативными актами.

Статьей 192 Трудового кодекса РФ от 30 декабря 2001 г. установлено, что за совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания:

1) замечание;
2) выговор;
3) увольнение по соответствующим основаниям.

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

Закон РФ “Об информации, информационных технологиях и о защите информации” от 27.13.2006г. № 149-ФЗ 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:

1. Основные понятия в области информации, и ее защиты.
2. Права обладателя информации.
3. Право на доступ и ограничения доступа к информации.
4. Использование информационно-телекоммуникационных сетей и государственное регулирование в этой сфере.

5. Защита информации, в том числе использование ЭЦП.

В законе даны определения:

информация – сведения (сообщения, данные) независимо от формы их представления (может являться объектом правовых отношений и свободно использоваться любым лицом за исключением ограничений, введенных законом);

конфиденциальность информации – обязательное требование не передавать такую информацию третьим лицам без согласия ее обладателя;

документированная информация – зафиксированная на материальном носителе информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления и распространения информации;

информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

информационная система – совокупность:

- информации, содержащейся в базах данных;
- информационных технологий, обрабатывающих информацию;
- технических средств, обеспечивающих обработку информации.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются *государственными информационными ресурсами*.

Электронное сообщение, подписанное электронной цифровой подписью, признается, равнозначным документу, подписанному собственноручной подписью.

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

Настоящий ФЗ регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Основные понятия, используемые в ФЗ:

- **информация** – сведения (сообщения, данные) независимо от формы их представления;
- **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- **информационно-телекоммуникационная сеть** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- **обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- **доступ к информации** – возможность получения информации и ее использования;
- **конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- **предоставление информации** – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

- **распространение информации** – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
- **электронное сообщение** – информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
- **документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- **оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

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

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

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

5. Режимы доступа к информации. Информация свободного доступа. Виды режимов ограниченного доступа.

Обладателем информации может быть физическое лицо, юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование. Обладатель информации вправе: -разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа; -использовать информацию, в том числе распространять ее, по своему усмотрению; -передавать информацию другим лицам по договору или на ином установленном законом основании; -защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Ограничение доступа к информации устанавливается в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Режимы доступа к информации

в соответствии с Законом РФ "Об информации, информационных технологиях и о защите информации" от 27.07.2006г. № 149-ФЗ и Указом Президента РФ № 188 от 6.03.1997г.

Режим доступа	Вид режима	Состав сведений
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

Режим ограниченного доступа

включает режим государственной тайны и режим конфиденциальности

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 вязи", "О банках и банковской деятельности", "О полиции" и др.

Режим общественного достояния создает условия для беспрепятственного ознакомления и использования соответствующих сведений. Так истечение срока действия исключительных прав на объекты интеллектуальной собственности (например, авторское право действует в течении всей жизни автора и 70 лет после

его смерти) означает переход их в общественное достояние. Произведение, перешедшее в общественное достояние, может свободно использоваться любым лицом без чьего-либо согласия или разрешения и без выплаты авторского вознаграждения. При этом охраняются авторство, имя автора и неприкосновенность произведения. (ГК РФ часть 4, ст. 1282)

Режим массовой информации распространяется на информацию в СМИ и различные публикации и отражает гарантируемую Конституцией РФ свободу массовой информации (ст. 29). Ограничения на публикуемые в СМИ сообщения даны в Конституции РФ Законе РФ «О средствах массовой информации» от 27 декабря 1991 года № 2124-1, (ред. от 16.10.2006 №160-ФЗ).

Режим исключительных прав – защита объектов интеллектуальной собственности. 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.

Режим ограниченного доступа включает *режим конфиденциальности и режим государственной тайны.*

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 вязи” , “О банках и банковской деятельности” , “О полиции” и др.

6. 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).

Другие лица не могут использовать соответствующий результат интеллектуальной деятельности или средство индивидуализации без согласия правообладателя, за исключением случаев, предусмотренных Гражданским кодексом. 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.

Режим исключительных прав – защита объектов интеллектуальной собственности. 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.

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

7. Конфиденциальность информации. Перечень сведений конфиденциального характера.

Информация - сведения (сообщения, данные) независимо от формы их представления (может являться объектом правовых отношений и свободно использоваться любым лицом за исключением ограничений, введенных законом);

Конфиденциальность информации - обязательное требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Сведения – Коммерческая, служебная и профессиональная тайны. Персональные данные. Тайна следствия и судопроизводства. Сведения о сущности неопубликованных изобретений

В отношении профессиональной тайны действуют нормы Закона “Об информации, информационных технологиях и о защите информации” (статья 9)

Профессиональная тайна - информация, полученная лицами при исполнении ими профессиональных обязанностей, подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Определение понятия «служебная тайна» дано в 1 части ГК РФ, в ст.139 “Служебная и коммерческая тайна”:

-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.

В отличии от профессиональной тайны служебная тайна связана с интересами государственной службы и службы в органах местного самоуправления.

8. Требования по безопасности компьютерных сетей в РФ.

Требования к безопасности компьютерных сетей в РФ разработаны Государственной технической комиссией РФ ныне ФСТЭК. Эти требования 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, следующие РД ГТК:

- «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» от 30.03.92 г.
- «Средства ВТ. Защита от НСД. Показатели защищенности от НСД к информации» от 30.03.92 г.
- «Защита от НСД к информации. Термины и определения». Решение Председателя ГТК от 30.03.92 г.
- «Концепция защиты СВТ и АС от НСД к информации». Решение Председателя ГТК от 30.03.92 г.
- «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники». Решение Председателя ГТК от 30.03.92 г.
- «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от несанкционированного доступа к информации». Решение Председателя ГТК от 25.07.97 г.
- «Специальные требования и рекомендации по технической защите конфиденциальной информации» от 2001г.

Государственное регулирование в сфере применения информационных технологий.

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 (ст. 15) соблюдения требований к распространению информации и охране объектов интеллектуальной собственности.

В ст. 15 закона “Об информации...” установлены нормы защиты прав пользователя информационными сетями. При использовании почтовых отправлений и электронных сообщений, отправитель информации обязан обеспечить получателю

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

Статья 10.1. Обязанности организатора распространения информации в сети "Интернет" Устанавливает требования: Организатор распространения информации в сети "Интернет" обязан обеспечивать реализацию требований к оборудованию и программно-техническим средствам, используемым им в эксплуатируемых информационных системах, для проведения органами, осуществляющими ОРД (Оперативно-разыскная деятельность), мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий.

9. 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. от 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.

Субъекты правоотношений:

- органы государственного управления;
- юридические лица, независимо от их организационно-правовых форм деятельности и видов собственности;
- граждане и должностные лица, которые взяли на себя обязательство либо обязаны по своему статусу выполнять требования законодательства о государственной тайне.

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

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.

10. 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. Степень секретности сведений, составляющих ГТ, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ вследствие распространения указанных сведений.

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

- "особой важности" (ОВ),
- "совершенно секретно" (СС),
- "секретно" (С).

ОВ – если при разглашении наносится ущерб интересам РФ;

СС – если при разглашении наносится ущерб интересам отрасли или министерства;

С – если при разглашении наносится ущерб интересам предприятия.

При засекречивании сведений их носителям присваивается соответствующий гриф секретности. Существует также промежуточный гриф для документов, которые не являются тайной предприятия, но не предназначены для открытого использования: ДСП – для служебного пользования. Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

На носители сведений, составляющих ГТ, наносятся реквизиты, включающие следующие данные:

- о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию,
- об органе государственной власти,

- о предприятии, об учреждении, организации, осуществивших засекречивание носителя,
- о регистрационном номере,
- о дате или условии рассекречивания сведений.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих ГТ, эти данные указываются в сопроводительной документации на этот носитель.

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

- *законности (*заключается в том, что засекречиванию не подлежат сведения, указанные в статье 7 закона о ГТ (которые раньше относились к ГТ)*),*
- *обоснованности (*заключается в установлении целесообразности засекречивания сведений по экономическим или иным критериям*),*
- *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 (Статья 7):

- 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 размерах золотого запаса и государственных валютных резервах;
- о состоянии здоровья высших должностных лиц;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

Виновные в нарушении требований закона должностные лица могут быть привлечены к уголовной, административной или дисциплинарной ответственности. Все граждане вправе обжаловать такие действия в суде.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью путем утверждения соответствующих перечней.

Обоснование необходимости отнесения сведений к ГТ в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Межведомственная комиссия по защите ГТ формирует, *Перечень сведений*, отнесенных к ГТ. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом РФ, подлежит открытому опубликованию и пересматривается по мере необходимости. *Перечень должностных лиц*, наделенных полномочиями по отнесению сведений к ГТ, утвержден распоряжением Президентом РФ от 30.05.97г. №226-рп «О перечне должностных лиц органов государственной власти, наделенных полномочиями по отнесению сведений к ГТ».

Должностные лица, наделенные полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся у собственника информации, если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к ГТ.

Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.

Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в соответствии с договором между органом государственной власти и ее собственником информации.

Не может быть ограничено право собственности на информацию иностранных юридических лиц и граждан, если она получена без нарушения законодательства РФ.

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

Основания для рассекречивания сведений:

- 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.

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

Режим защиты государственных секретов обеспечивается уполномоченными органами. Эти органы организуют и обеспечивают защиту информации, содержащей ГТ в соответствии с функциями, возложенными на них законодательством РФ. Органы защиты государственной тайны:

- межведомственная комиссия по защите ГТ;
- ФСБ,
- МО (министерство обороны),
- СВР (служба внешней разведки),
- ФСТЭК.

Допуск должностных лиц и граждан к ГТ предусматривает:

- принятие на себя обязательств перед государством по нераспространению сведений, составляющих ГТ;
- согласие на частичные, временные ограничения их прав в соответствии со статьей 24 настоящего Закона;

- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления льгот, предусмотренных настоящим Законом;
- ознакомление с нормами законодательства РФ о ГТ, предусматривающими ответственность за его нарушение;
- принятие решения руководителем органа государственной власти или предприятия, о допуске 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 «ОВ»

Вторая – к сведениям «СС»

Третья – к сведениям «С»

Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности. Сроки, обстоятельства и порядок переоформления допуска граждан к ГТ устанавливаются нормативными документами Правительством РФ. Порядок допуска должностных лиц и граждан к ГТ в условиях объявленного чрезвычайного положения может быть изменен Президентом 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, предусмотренных статьей 21 Закона.

Особый порядок допуска к ГТ имеют. Указанные лица предупреждаются о неразглашении ГТ, ставшей им известной в связи с исполнением ими своих полномочий, и о привлечении их к ответственности в случае ее разглашения, о чем

у них отбирается соответствующая расписка. Сохранность ГТ в таких случаях гарантируется путем установления ответственности указанных лиц федеральным законом.

Должностное лицо или гражданин, допущенные к ГТ, могут быть временно ограничены в следующих правах:

- права выезда за границу на срок, оговоренный в трудовом договоре при оформлении допуска к ГТ;
- права на распространение сведений, составляющих ГТ, и на использование открытий и изобретений, содержащих такие сведения;
- права на неприкосновенность частной жизни при проведении проверочных мероприятий.

Допуск должностного лица или гражданина к ГТ может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях:

- расторжения с ним трудового договора в связи с проведением организационных и (или) штатных мероприятий,
- однократного нарушения им взятых на себя предусмотренных трудовым договором обязательств, связанных с защитой ГТ,
- возникновения обстоятельств, являющихся основанием для отказа должностному лицу или гражданину в допуске к ГТ,
- прекращение допуска должностного лица или гражданина к ГТ является дополнительным основанием для расторжения с ним трудового договора, если такие условия предусмотрены в трудовом договоре.

Прекращение допуска к ГТ не освобождает должностное лицо или гражданина от взятых ими обязательств по неразглашению сведений, составляющих ГТ. Решение администрации о прекращении допуска должностного лица или гражданина к ГТ и расторжении на основании этого с ним трудового договора может быть обжаловано в вышестоящую организацию или в суд.

Допуск предприятий и организаций к проведению работ, связанных с использованием сведений, составляющих ГТ, с созданием средств защиты

информации, а также с осуществлением мероприятий и оказанием услуг по защите ГТ, осуществляется путем получения ими, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих ГТ (ст. 27).

Лицензия на проведение работ с использованием сведений, составляющих ГТ, выдается предприятию, учреждению, организации при выполнении ими следующих условий (ст. 27):

- выполнение требований, утверждаемых Правительством РФ, по обеспечению защиты ГТ;
- наличие в их структуре подразделений по защите ГТ и специально подготовленных сотрудников для работы по защите информации;
- наличие у них сертифицированных средств защиты информации.

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на ФСБ, МО, ФСТЭК. Сертификация осуществляется на основании требований государственных стандартов РФ и иных нормативных документов, утверждаемых Правительством РФ.

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, определяется Уголовным кодексом РФ:

- ст. 275. Государственная измена – Государственная измена, то есть шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности РФ, совершенная гражданином РФ, - наказывается лишением свободы на срок от двенадцати до двадцати лет со штрафом в размере до пятисот тысяч рублей,

- ст. 276. Шпионаж – Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих ГТ, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности РФ, если эти деяния совершены иностранным гражданином или лицом без гражданства, - наказываются лишением свободы на срок от десяти до двадцати лет,

- ст. 283. Разглашение государственной тайны – Разглашение сведений, составляющих ГТ, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены - наказывается арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет. То же деяние, с тяжкими последствиями - наказываются лишением свободы от трех до семи лет с лишением права занимать определенные должности на срок до трех лет,

- ст. 284. Утрата документов, содержащих ГТ – Нарушение лицом, имеющим допуск к ГТ, установленных правил обращения с содержащими ГТ документами, если это повлекло по неосторожности их утрату и наступление тяжких последствий - наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет.

За обеспечением защиты ГТ установлен (ст. 30 и 32 закона) *ведомственный контроль*. Его осуществляют Органы государственной власти, наделенные в соответствии с настоящим Законом полномочиями по распоряжению сведениями,

составляющими ГТ, обязаны контролировать эффективность защиты этих сведений во всех подчиненных и подведомственных их органах государственной власти, на предприятиях, в учреждениях и организациях, осуществляющих работу с ними.

Межведомственный контроль осуществляют:

- федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности,
- федеральный орган исполнительной власти, уполномоченный в области обороны,
- федеральный орган исполнительной власти, уполномоченный в области внешней разведки,
- федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы, на которые эта функция возложена законодательством РФ.

За обеспечением защиты ГТ установлен Контроль за обеспечением защиты ГТ. Его осуществляют Президент и Правительство РФ. Надзор за соблюдением законодательства осуществляют Генеральный прокурор РФ и подчиненные ему прокуроры.

12.Сведения, составляющим КТ. Виды конкурентной разведки.

Определение понятия «служебная тайна» дано в 1 части ГК РФ, в ст.139 “Служебная и коммерческая тайна”:

-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.

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. 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. 4

3. Выполнение услуг охраны и сыска, предусмотренных Законом "О частной детективной и охранной деятельности ".

4. Сбор информации маркетингового характера. Именно это направление понимается на Западе под конкурентной разведкой.

Виды конкурентной разведки (сбор информации маркетингового характера):

наблюдение;

отчеты торговых работников;

поиск информации в открытых БД;

анализ годовых отчетов предприятий;

обратный инжиниринг.

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

Определение понятия «служебная тайна» дано в 1 части ГК РФ, в ст.139 “Служебная и коммерческая тайна”:

-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.

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. Принято различать: конкурентную разведку ("деловая разведка", "бизнес-разведка") и промышленный шпионаж.

Правовая охрана служебной и коммерческой тайны предполагает подготовку необходимой документации для организации доступа к информации. Нужно

установить круг лиц, имеющих доступ к засекреченным сведениям, определить порядок обращения к информации и контроль за его соблюдением.

Все лица, которые имеют доступ к коммерческой тайне, должны подписать соответствующие документы, определяющие обязательства по неразглашению и ответственность за нарушение обязательств.

К категории коммерческой тайны **НЕ относятся** общедоступные сведения типа юридического адреса или учредительных документов, а также информация:

о загрязнении окружающей среды;

о численности и составе сотрудников;

о задолженности работодателей по выплате зарплаты и по иным социальным выплатам;

о нарушениях законодательства России и фактах привлечения к ответственности за совершение этих нарушений;

о перечне лиц, имеющих право действовать без доверенности от имени юридического лица.

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

Определение понятия «служебная тайна» дано в 1 части ГК РФ, в ст.139 “Служебная и коммерческая тайна”:

-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.

Для создания правовых основ защиты информации на коммерческом предприятии необходимо:

1.Ввести в Устав предприятия в раздел “Права и обязанности предприятия”:

“Предприятие имеет право определять состав, объем и порядок защиты сведений, составляющих КТ, требовать от сотрудников предприятия обеспечения ее сохранности”. “Предприятие обязано обеспечить сохранность КТ”.

Внесение этих требований дает право администрации предприятия: -создавать организационные структуры по защите КТ; -издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих КТ, и механизмы ее защиты; -включать требования по защите КТ в договора по всем видам хозяйственной деятельности; -требовать защиту интересов предприятия перед государственными и судебными органами.

Администрация предприятия обязуется обеспечить разработку и осуществление мероприятий по введению режима и защите КТ

СБ для сохранения КТ принимает меры по

¬максимальному ограничению круга лиц, допускаемых к КТ;

¬ физической сохранности документов, содержащих такие сведения;

¬обработки информации с грифом «КТ» на защищенных ЭВМ;

¬внесению требований по конфиденциальности конкретной информации в договоры с внутренними и внешнеторговыми партнерами, а также проводит другие мероприятия по решению руководства.

Ответственность за разглашение «служебной тайны» дана в ст.139 части первой ГК РФ “Служебная и коммерческая тайна”:

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки.

Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

15. 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:

1.Устав предприятия;

2.Коллективный договор предприятия;

3.Трудовые и гражданско-правовые договора;

4.Правила внутреннего трудового распорядка рабочих и служащих предприятия;

5.Должностные обязанности руководителей, специалистов, рабочих и служащих предприятия. и другие документы.

Для создания правовых основ защиты информации на коммерческом предприятии необходимо: 1. Ввести в Устав предприятия в раздел “Права и обязанности предприятия”:

“Предприятие имеет право определять состав, объем и порядок защиты сведений, составляющих КТ, требовать от сотрудников предприятия обеспечения ее сохранности”. “Предприятие обязано обеспечить сохранность КТ”.

Внесение этих требований дает право администрации предприятия:

- создавать организационные структуры по защите КТ;

- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих КТ, и механизмы ее защиты; -включать требования по защите КТ в договора по всем видам хозяйственной деятельности;

- требовать защиту интересов предприятия перед государственными и судебными органами.

2. Разработать “Перечень сведений, составляющих КТ предприятия” и довести его под роспись до всех сотрудников.

3. Дополнить “Коллективный договор” следующими требованиями:

- В раздел “Предмет договора” Администрация предприятия обязуется обеспечить разработку и осуществление мероприятий по введению режима и защите КТ. Трудовой коллектив принимает на себя обязательство по соблюдению установленных на предприятии требований по защите КТ.

- В раздел “Кадры” Администрация обязуется привлекать нарушителей требований по защите КТ к административной и уголовной ответственности в соответствии с действующим законодательством.

4. Дополнить правила внутреннего распорядка дня работников требованиями о неразглашении КТ. При поступлении рабочего или служащего на работу, переходе его на другую работу а также при увольнении, администрация обязана проинструктировать работника по правилам сохранения КТ с оформлением письменного обязательства о ее неразглашении.

5. Ввести в текст трудового договора требования по защите КТ. Тогда независимо от формы заключения договора (устная или письменная) подпись работника на приказе о приеме на работу подтверждает его согласие с условиями договора. Если договор заключается в устной форме, то действует требование по защите КТ, вытекающее из правил внутреннего трудового распорядка.

6. В должностные обязанности руководителей, специалистов, рабочих и служащих записать, что:

- сотрудники должны знать относящиеся к их деятельности сведения, являющиеся КТ, выполнять лично требования по ее защите и принимать меры по предупреждению нарушений установленных норм сохранности КТ. Включение этих требований дает право администрации предприятия применять к нарушителям меры дисциплинарного воздействия в соответствии с Трудовым кодексом РФ.

Руководителю предприятия, при создании системы безопасности на своей фирме, необходимо определить следующее:

- какая информация нуждается в защите;
- кого она может заинтересовать;
- каков “срок жизни” этих секретов;
- во что обойдется их защита.

В рамках режима КТ на предприятии вводятся система закрытого делопроизводства.

Целям защиты информации, обрабатываемой в АС служит принятый 2002 г. Закон РФ «Об электронной цифровой подписи» (в ред ФЗ "Об электронной подписи" от 6 апреля 2011 г. N 63-ФЗ)

ЭЦП – реквизит документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе (ст. 3) признается равнозначной собственноручной подписи лица на бумажном носителе, заверенном печатью (ст. 19).

16.Виды угроз информации в автоматизированных системах. Ответственность за компьютерные преступления.

Средства автоматизированной обработки информации с использованием ЭВМ имеют ряд особенностей, дающих широкие возможности для злоумышленных действий.

Можно выделить следующие виды угроз информации в АС:

1.Перехват информации:

- по электромагнитному излучению (излучения ЭЛТ можно принимать на расстояниях до 1000 м.);
- по виброакустическому каналу (таблетки, клопы, жучки, через несущие конструкции и проемы здания, стетоскоп);
- видеоперехват (бинокль, фото- и видеокамеры);
- использование отходов информационного процесса (физические – дискеты, пленки и “мусор” в памяти компьютера).

2.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 – вскрывается 42% паролей из 8 символов.

3.Манипуляция данными и управляющими командами:

- умышленное изменение данных;
- изменение логических связей в электронных цепях и топологии микросхем.

4.Компьютерные вирусы.

“Троянский конь” – программа выдает себя за известную

“Троянская матрешка” – программа создает “троянского коня” и самоуничтожается.

“Троянский червь” – реализуется саморазмножения.

“Логическая бомба” – программа активируется при стечении определенных обстоятельств (включает алгоритм “троянского коня”) или в определенный момент времени “временная бомба”.

“Воздушный змей” переброска средств с одного счета на другой и обратно с постепенным увеличением сумм.

5.Использование специальных программных средств:

- “моделирование” процессов и способов преступления путем создания игровой программы защита-преодоление.

6.Комплексные методы. Использование двух и более способов и их комбинации.

Эффективная борьба с КП в РФ ведется с 1997г. после принятия УК РФ, в котором помещена глава 28 «Преступления в сфере компьютерной безопасности».

Составы компьютерных преступлений даны в следующих статьях:

- «Неправомерный доступ к компьютерной информации» (ст. 272);

1. Неправомерный доступ к компьютерной информации, то есть информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, или их сети, – наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное организованной группой либо лицом с использованием своего служебного положения, имеющим доступ к ЭВМ, – наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

- «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273);

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

- «Нарушение правил эксплуатации ЭВМ» (ст. 274).

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

17.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.

Деятельность СБ должна быть основана на государственных и внутрифирменных нормативных документах.

Законы РФ: «О частной детективной и охранной деятельности» от 11.3.1992 №2487-1, ред. от 10.01.2003 №15-ФЗ, «О безопасности» от 5.3.1992 №2446-1, «Об оружии» от 13.12.1996 №150-ФЗ, «Об информации…» от 27.13.2006 № 149-ФЗ, «О ведомственной охране» от 14.4.1999 №77-ФЗ, ГК РФ и Трудовой Кодекс.

Постановления Правительства РФ: «Вопросы частной детективной и охранной деятельности» от 14.8.1992 №587, «Об организации ведомственной охраны» от 12.7.2000 №514.

Внутренние документы:

- Устав фирмы, трудовые договоры, правила внутреннего трудового распорядка, должностные обязанности руководителей, специалистов, рабочих и служащих, положение о СБ;
- инструкция по организации режима и охраны;
- инструкция по защите КТ;
- перечень сведений, составляющих КТ;
- инструкция по работе с конфиденциальной информацией для руководителей, специалистов и технического персонала;
- инструкция по хранению документов, содержащих КТ в архиве;
- инструкция по инженерно-технической защите информации;
- инструкция о порядке работы с иностранными представителями.

Основным документом, регулирующим вопросы создания и деятельности СБ, является Закон РФ «О частной детективной и охранной деятельности», №2487-1 от 11.03.92г. (ред. от 07.02.2011 N 4-ФЗ) Основные положения:

➢ Частная детективная и охранная деятельность осуществляется физическими и юридическими лицами, имеющими специальное разрешение (лицензию) (ст.1,4), которая выдается органом внутренних дел (лица, занимающиеся частной детективной деятельностью, не вправе осуществлять оперативно – розыскные действия).

➢ Предприятия, независимо от организационно-правовых форм, вправе учреждать обособленные подразделения (службы безопасности) для осуществления охранно-сыскной деятельности в интересах собственной безопасности учредителя (ст.14).

В целях сыска разрешается предоставление следующих 7 видов услуг (ст. 3):

➢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.

При осуществлении частной сыскной деятельности допускается (ст. 5):

➢использование видео- и аудиозаписи, кино- и фотосъемки,

➢технических и иных средств, не причиняющих вреда жизни и здоровью граждан и окружающей среде,

➢средств оперативной радио- и телефонной связи,

➢устный опрос граждан и должностных лиц (с их согласия), наведение справок, изучение предметов и документов (с письменного согласия их владельцев), внешний осмотр строений, помещений и других объектов.

Частным детективам запрещается (ст. 7):

➢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 (ст. 12).

Лицензия НЕ ВЫДАЕТСЯ (ст. 6):

1) гражданам, не достигшим двадцати одного года;

2) гражданам, состоящим на учете в органах здравоохранения по поводу психического заболевания, алкоголизма или наркомании;

3) гражданам, имеющим судимость за совершение умышленного преступления;

4) гражданам, которым предъявлено обвинение в совершении преступления (до разрешения вопроса об их виновности в установленном законом порядке);

5) гражданам, уволенным с государственной службы, из судебных, прокурорских и иных правоохранительных органов по компрометирующим их основаниям;

6) бывшим работникам правоохранительных органов, осуществлявшим контроль за частной детективной и охранной деятельностью, если со дня их увольнения не прошел год;

7) гражданам, не представившим документы, перечисленные в части второй настоящей статьи.

Продление срока действия удостоверения частного охранника осуществляется только после повышения квалификации в образовательных учреждениях (ст. 11).

Частная охранная организация может быть создана только в форме общества с ограниченной ответственностью и не может осуществлять иную деятельность, кроме охранной (ст. 15).

Руководитель частной охранной организации должен иметь высшее профессиональное образование и пройти повышение квалификации для руководителей частных охранных организаций.

Обязательное требование – наличие у руководителя частной охранной организации удостоверения частного охранника (ст. 15).

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.

Охранник при применении специальных средств или огнестрельного оружия обязан:

➢предупредить о намерении их использовать;

➢стремиться, чтобы любой ущерб, причиненный при устранении опасности, был минимальным;

➢немедленно уведомить прокурора о всех случаях смерти или причинения телесных повреждений.

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 ТУ 6- 02-832-76;

➢ газовый пистолет ТУ БВ-Г.000;

➢ наручники ТУ 87.2.026-88;

➢ палка резиновая (пластиковая).

Виды вооружения охранников, (порядок приобретения, учета, хранения и ношения оружия регламентируются Правительством РФ):

➢ 9мм пистолет ПМ ТУ 9375-88;

➢ ружье охотничье гладкоствольное ТУ 3-3.1421-83;

➢ боеприпасы к оружию ТУ А9003-80.

Частные детективы и охранники обязаны проходить периодическую проверку на пригодность к действиям в условиях, связанных с применением специальных средств и огнестрельного оружия, определяемой МВД.

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 (ст. 18):

1) специальные средства в следующих случаях:

➢для отражения нападения;

➢для пресечения преступления, когда правонарушитель оказывает физическое сопротивление.

2) огнестрельное оружие

➢для отражения нападения;

➢для предупреждения (выстрелом в воздух).

Контроль и надзор за частной детективной и охранной деятельностью (ст. 20).

Контроль за частной детективной и охранной деятельностью осуществляют Министерство внутренних дел.

Надзор за исполнением настоящего Закона осуществляют Генеральный прокурор РФ и подчиненные ему прокуроры.

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

В *целях сыска* разрешается предоставление следующих 7 видов услуг (ст. 3):

➢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.

При осуществлении частной сыскной деятельности допускается (ст. 5):

➢использование видео- и аудиозаписи, кино- и фотосъемки,

➢технических и иных средств, не причиняющих вреда жизни и здоровью граждан и окружающей среде,

➢средств оперативной радио- и телефонной связи,

➢устный опрос граждан и должностных лиц (с их согласия), наведение справок, изучение предметов и документов (с письменного согласия их владельцев), внешний осмотр строений, помещений и других объектов.

Частным детективам запрещается (ст. 7):

➢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 (ст. 12).

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.

УК РФ. Статья 203. *Превышение полномочий* частным детективом или работником частной охранной организации, имеющим удостоверение частного охранника, при выполнении ими своих должностных обязанностей

1. 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, 30 либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет.

2. То же деяние, совершенное с применением насилия или с угрозой его применения либо с использованием оружия или специальных средств и повлекшее тяжкие последствия, - наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

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

Перечень специальных технических средств (СТС), утвержденных постановлением Правительства РФ от 1 июля 1996 г. № 770:

1. СТС для негласного получения и регистрации акустической информации.
2. СТС для негласного визуального наблюдения и документирования.
3. СТС для негласного прослушивания телефонных переговоров.
4. СТС для негласного перехвата и регистрации информации с технических каналов связи.
5. СТС для негласного контроля почтовых сообщений и отправлений.
6. СТС для негласного исследования предметов и документов.

7. СТС для негласного проникновения и обследования помещений, транспортных средств и других объектов.

8. СТС для негласного контроля за перемещением транспортных средств и других объектов.

9. СТС для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.

10. СТС для негласной идентификации личности. Ответственность за данные нарушения указана в статьях УК РФ.

Частным детективам запрещается проведение оперативно-розыскных мероприятий и использование специальных и иных технических средств, предназначенных для негласного получения информации.

УК РФ Статья 138. *Нарушение тайны переписки*, т*елефонных переговоров, почтовых, телеграфных или иных сообщений*

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

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до шести месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года.

2. То же деяние, совершенное лицом с использованием своего служебного положения, –

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 лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо принудительными работами на срок до четырех лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до четырех лет.

УК РФ. Статья 203. *Превышение полномочий* частным детективом или работником частной охранной организации, имеющим удостоверение частного охранника, при выполнении ими своих должностных обязанностей

1. 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, 30 либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет.

2. То же деяние, совершенное с применением насилия или с угрозой его применения либо с использованием оружия или специальных средств и повлекшее тяжкие последствия, - наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

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

Указ Президента РФ №21 от 9.01 96г. «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в РФ и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» постановляет возложить на ФСБ:

➢ выдачу разрешений на деятельность и контроль использования в области специальных технических средств, предназначенных для негласного получения информации ;

➢ лицензирование деятельности не уполномоченных на осуществление оперативно-розыскной деятельности физических и юридических лиц, связанной с

разработкой, производством, реализацией, приобретением в целях продажи, ввозом в РФ и вывозом за ее пределы специальных технических средств, предназначенных для негласного получения информации, а также сертификацию, регистрацию и учет таких специальных технических средств;

➢ выявление и пресечение случаев проведения оперативно- розыскных мероприятий и использования специальных и иных технических средств, разработанных, приспособленных, запрограммированных для негласного получения информации, неуполномоченными лицами.

Постановлением Правительства от 1.07.96г. №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.

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

Для обеспечения защиты ГТ и СТ (в важных для страны областях) действует Государственная система защиты информации в РФ (ГСЗИ), которая включает:

- совокупность органов (ФСБ, ФСТЭК, СБ), сил и средств, осуществляющих деятельность в области защиты информации (ЗИ);
- систему лицензирования деятельности в области ЗИ;
- систему сертификации средств ЗИ;
- систему 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 – это 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;

а также подготовка и переподготовка кадров.

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

З*аконодательной и нормативной базой лицензирования и сертификации* в области ЗИ являются Законы РФ:

-"О государственной тайне" от 21.07.93 №5485-1;

-"О техническом регулировании" от 27 декабря 2002 г. N 184-ФЗ

-"О лицензировании отдельных видов деятельности", от 8.08 2001г. №128 (ред. от 11.03.2003г. №32);

-"О защите прав потребителей" от 07.02.92 №2300-1;

Постановления Правительства РФ:

-"О лицензировании отдельных видов деятельности" от 24 12 94 №1418;

-"О лицензировании деятельности предприятий..." от 15.04.95 №333;

-"О сертификации средств ЗИ" от 26.06.95 №608.

-“О лицензировании… от 27.05.2002 №348.

-“О лицензировании… от 30.04.2002 №290, (ред. №64 от 6.02.2003). А также Указы Президента РФ, и ряд других подзаконных актов.

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

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;

а также подготовка и переподготовка кадров.

Постановлением Правительства РФ №333 утверждено Положение о лицензировании деятельности предприятий, в котором установлено, что:

- лицензия разрешает осуществление конкретного вида деятельности в течение установленного срока на всей территории Российской Федерации, а также в учреждениях Российской Федерации, находящихся за границей;
- органами, уполномоченными на ведение лицензионной деятельности, являются:
- по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих ГТ – ФСБ, СВР(за рубежом);
- на право проведения работ, связанных с созданием средств защиты информации - ФСТЭК, ФСБ в пределах их компетенции;
- на право осуществления мероприятий и (или) оказания услуг в области защиты ГТ – ФСБ и ее территориальные органы, ФСТЭК, СВР (в пределах их компетенции)

В соответствии законом *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.

В новой редакции закона «О лицензировании отдельных видов деятельности» добавлены следующие виды деятельности:

► деятельность по изготовлению экземпляров аудиовизуальных произведений, программ для ЭВМ, баз данных и фонограмм на любых видах носителей;

► образовательная деятельность;

► частная охранная деятельность;

► частная детективная (сыскная) деятельность;

► оказание услуг связи.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не может быть менее трех и более пяти лет.

Для получения лицензии предприятие обязано предъявить следующий перечень документов. К заявлению на получение лицензии необходимо приложить следующие документы:

- копия свидетельства о государственной регистрации предприятия;
- копии учредительных документов, заверенных нотариусом;
- копии документов на право собственности или аренды имущества, необходимого для ведения заявленной деятельности;
- справка налогового органа о постановке на учет;
- представление органов государственной власти РФ с ходатайством о выдаче лицензии;
- документ, подтверждающий оплату рассмотрения заявления.

Проведение экспертизы осуществляется экспертными комиссиями Лицензионного центра либо Аттестационными центрами.

Заявление о предоставлении лицензии и прилагаемые к нему документы соискатель лицензии вправе направить в лицензирующий орган как почтовым отправлением, так и в форме электронного документа, подписанного ЭЦП.

В этом случае лицензирующий орган направляет соискателю лицензии в форме электронного документа, подписанного ЭЦП.

На каждый вид деятельности предоставляется лицензия, которая действует бессрочно. В 4-х последних случаях срок ее действия может устанавливаться федеральными законами (ст. 1).

В ст. 14 закона дан порядок принятия решения о предоставлении лицензии или об отказе. Решение принимается в течение 45 дней. В течение 3-х дней после подписания, лицензия вручается или направляется по почте лицензиату. Проводятся плановые проверки лицензиата Основания для их проведения:

➢ истечение 1 года после предоставления лицензии,

➢ истечение 3-х лет после последней проверки.

А также внеплановые проверки.

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

Национальный орган по сертификации определяется Правительством РФ. В настоящее время эти функции выполняет Федеральное агентсво по техническому регулированию и метрологии (ФАТРиМ).

В 1994 г. Были 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 торговли;

● 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.

Сертификация осуществляется на основании требований государственных стандартов РФ и иных нормативных документов, утверждаемых Правительством РФ.

Положение о сертификации средств ЗИ утверждено постановлением Правительства РФ от 25.06.95 г. № 608 (в ред. ПП РФ N 509 от 23.04.96) и зарегистрировано Госстандартом России в Государственном реестре 20 марта 1995 г. (Свидетельство № РОСС RU. 0001. 01БИ00).

Порядок сертификации:

1.В Центральный орган по сертификации подается заявление и полный комплект технической документации.

2.Центральный орган назначает испытательный центр (лабораторию) для проведения испытания.

3.Испытания проводятся на основании хозяйственного договора между заявителем и испытательным центром.

4.Сертификация (экспертиза материалов и подготовка документов для выдачи) осуществляется Центральным органом.

Сертификат выдается на срок до 5 лет

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:

1.Сертификация изделий, обеспечивающих защиту ГТ является обязательной.

2.Обязательность использования криптографических алгоритмов, являющихся стандартами.

3.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.

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

Лицензирование деятельности в области защиты конфиденциальной информации основано на Законе РФ «О лицензировании отдельных видов деятельности» от 8 августа 2001 г. № 128-ФЗ (ред. от 4 мая 2011 г. № 99-ФЗ).

Действие данного закона НЕ РАСПРОСТРАНЯЕТСЯ на следующие виды деятельности, связанные с ЗИ:

► деятельность, связанная с защитой государственной тайны;

► деятельность в области связи;

► использование результатов интеллектуальной деятельности.

Постановление Правительства РФ от 3.02.2012 г. № 79 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 (ТЗКИ) понимается комплекс мероприятий по ее защите от несанкционированного доступа в целях ее уничтожения, искажения или блокирования доступа к ней.

Лицензирование работ по ТЗКИ осуществляет ФСТЭК.

Постановление Правительства от 3.03.2012 г. № 171 утвердило "Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации".

Положение определяет порядок лицензирования данной деятельности, осуществляемой юридическими лицами и индивидуальными предпринимателями.

Лицензирование деятельности осуществляет ФСТЭК, а в части средств защиты конфиденциальной информации, устанавливаемых на объектах Администрации Президента РФ, Совета Безопасности РФ, Федерального Собрания РФ, Правительства РФ, Конституционного, Верховного и Высшего Арбитражного Суда РФ – ФСБ.

Для получения лицензии соискатель лицензии направляет в лицензирующий орган следующие документы:

а) заявление о предоставлении лицензии и другие указанные в законе документы;

б) копии документов, подтверждающих квалификацию специалистов;

в) копии документов, подтверждающих право собственности, либо копии договоров аренды помещений;

г) копии документов, подтверждающих право на используемые программы для электронно-вычислительных машин и базы данных;

д) сведения о наличии необходимого производственного, испытательного и контрольно-измерительного оборудования;

е) сведения об имеющихся у соискателя нормативных правовых актах, по вопросам разработки и производства средств защиты информации.

Лицензирующий орган принимает решение о предоставлении или об отказе в предоставлении лицензии в срок, не превышающий 45 дней с даты поступления в лицензирующий орган заявления.

Приказом ФСБ от 1 апреля 2009 г. № 123 утвержден регламент ФСБ РФ по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации.

Регламент определяет сроки и последовательность действий по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации.

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

25. Правовые основы деятельности органов, занимающихся оперативно-розыскной деятельностью. Виды ОРМ и условия проведение ОРМ, ограничивающих конституционные права человека.

Правовые основы:

- Деятельность этих органов основывается на Законе РФ “Об оперативно-розыскной деятельности”, от 12.08.95г. №144-ФЗ (ред. от 22.08.2004 №122-ФЗ).

Еще важно знать, что ОРМ - 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

ОРМ могут проводить органы: ФСБ,ОВД, Служба внешней разведки, органы по контролю оборотов наркотиков и т.д.

Виды ОРМ:

О*перативно-розыскные действия* – это простая форма ОРМ. К ним относятся оперативный опрос, наведение справок, наблюдение, оперативное отождествление, сбор образцов, исследование документов и предметов. При определенных обстоятельствах уровень действия может быть повышен до оперативно-розыскного мероприятия или оперативно-розыскной операции.

Оперативно-розыскное мероприятие рассматривается как совокупность отдельных оперативно-розыскных действий. К собственно ОРМ относятся контроль почтовых отправлений, оперативный осмотр, оперативный эксперимент, слуховой контроль, проверочная закупка, контроль в сетях электросвязи.

Оперативно-розыскные операции – самая сложная форма совокупность мероприятий и действия. К ним относятся оперативное внедрение и контролируемая поставка.

Условия проведения ОРМ:

1.Наличие возбужденного уголовного дела.

2.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.

3.Поручения следователя, указания прокурора или определения суда по уголовным делам, находящимся в их производстве.

4.Запросы других органов, осуществляющих оперативно- розыскную деятельность, по основаниям, указанным в настоящей статье.

5.Постановление о применении мер безопасности в отношении защищаемых лиц.

6.Запросы международных правоохранительных организаций и правоохранительных органов иностранных государств в соответствии с международными договорами РФ.

Проведение ОРМ, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, 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, создающих угрозу государственной, военной, экономической или экологической безопасности РФ.

4. В случаях, которые не терпят отлагательства и могут привести к совершению тяжкого преступления на основании мотивированного постановления одного из руководителей органа, осуществляющего ОРД, допускается проведение ОРМ, с обязательным уведомлением суда (судьи) в течение 24 часов.

26. 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. Это закон “Об органах ФСБ в РФ” от 3.04.95г. №40-ФЗ.

Также есть Закон РФ “О полиции”, №3 ФЗ от 07 февраля 2011 г.

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).

Контроль за деятельностью полиции (ст. 37), 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 (ст. 38).

Законом определено (ст. 11), 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.

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

Закон РФ “О банках и банковской деятельности” **устанавливает**, **что кредитная организация**, Банк России **гарантируют тайну** об операциях, о счетах и вкладах своих клиентов и корреспондентов.

Закон РФ “О конкуренции и ограничении монополистической деятельности на товарных рынках”, №948-1 от 22 марта 1991 г. (В ред.от 26.07.2006 № 135-ФЗ.) В соответствии с этим законом **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.

Закона РФ “О санитарно-эпидемиологическом благополучии населения”, от 30.03.99 №52-ФЗ (Ред. 8.11.2007 г. N 258-ФЗ)

Должностные лица, осуществляющие государственный санитарно-эпидемиологический надзор, обязаны соблюдать государственную, врачебную и иную охраняемую законом тайну в отношении информации, ставшей им известной при выполнении своих служебных обязанностей, и несут ответственность за ненадлежащее исполнение своих служебных обязанностей.

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

Три формы правовой защиты ИС:

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).

Интеллектуальная собственность – это результаты интеллектуальной деятельности (РИД) и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана. Это легальное определение, которое содержится в статье 1225 Гражданского кодекса РФ. Сюда относится:

авторское право, смежные права (исполнения и фонограммы), патентное право, средства индивидуализации (товарные знаки), секреты производства (ноу-хау).

Права на ИС могут быть:

исключительные (имущественные) – распоряжение изобретенным имуществом как вздумается

личные неимущественные – разрешение на публикацию своих трудов и т.д

иные – все что не входит в первые два права (например – право получения вознаграждения за труды)

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

Коммерческая тайна – связанная с производственной, технической, технологической информацией, управлением финансовой и другой деятельностью

предприятия, разглашение (передача, утечка) которой может нанести ущерб его интересам.

Законодательная база для взаимодействия с правоохранительными органами и органами контроля:

Закон РФ “О защите конкуренции” 26 июля 2006 года № 135-ФЗ.

Также есть Закон РФ “О полиции”, №3 ФЗ от 07 февраля 2011 г.

Одной из форм недобросовестной конкуренции является, согласно закона “О защите конкуренции”, получение, использование, разглашение научно-технической, производственной или торговой информации, в том числе КТ без согласия ее законного владельца (ст.14). К числу контролирующих органов относится федеральный антимонопольный орган, который имеет свои территориальные управления.

Вместе с тем и сам антимонопольный орган, располагая для выполнения возложенных функций значительными полномочиями (беспрепятственный доступ в органы управления, на предприятия, право на ознакомление со всеми необходимыми документами и др.), имеет и серьезные обязанности. Одна из них - по соблюдению 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. **За разглашение информации, составляющей коммерческую, служебную, иную охраняемую законом тайну, работники антимонопольного органа несут гражданско-правовую, административную и уголовную ответственность.**

Теперь о полиции:

Законом определено (ст. 11), что сотрудники милиция 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.

Поэтому собственник или его представитель вправе потребовать от работника милиции сведений, объясняющих необходимость вхождения на предприятие (или иной объект, например, факт возбуждения уголовного дела либо получения сведений при расследовании иного дела, его номер и орган, осуществляющий расследование). Осмотр производственных, складских, торговых и иных служебных помещений, транспортных средств, других мест хранения и использования имущества производится только с участием собственника либо его представителей или уполномоченных им лиц.

Надзор за законностью законностью деятельности полиции выполняет **генеральный прокурор**.

30.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".

Статья 10.1. Обязанности организатора распространения информации в сети "Интернет "

Устанавливает требования:

Организатор распространения информации в сети "Интернет" обязан обеспечивать реализацию требований к оборудованию и программно-техническим средствам, используемым им в эксплуатируемых информационных системах, для проведения органами, осуществляющими ОРД, мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий.

Неисполнение организатором распространения информации в сети "Интернет" **установленной** федеральным законом **обязанности** хранить и (или**) предоставлять** уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, **информацию о фактах** приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных **сообщений пользователей сети "Интернет"** и информацию о таких

пользователях - **влечет** наложение **административного штрафа** на граждан в размере от трех тысяч **до пяти тысяч рублей**; на должностных лиц - от тридцати тысяч **до пятидесяти тысяч рублей**; на юридических лиц - от трехсот тысяч **до пятисот тысяч рублей**.

31.Правовая защита профессиональной и служебной тайны в РФ. Виды профессиональной и служебной тайн.

Профессиональная тайна

Виды:

Врачебная тайна

- Адвокатская тайна
- Тайна исповеди
- Тайна связи
- Тайна усыновления
- Журналистская тайна
- Нотариальная тайна
- Тайна страхования

Законы РФ:

"Основы законодательства РФ о нотариате"

"О СМИ"

"Семейный кодекс РФ" - (Тайна усыновления – уголовная ответственность за разглашение)

"О связи" - (Тайна связи – уголовная ответственность за разглашение).

"Об утверждении положения (Нет доступа со стороны государства об адвокатуре РФ" - венных органов к адвокатской тайне).

"О религиозных объединениях" -(Нет доступа со стороны государственных органов к тайне исповеди).

Должностная служебная тайна связана с интересами государственной службы и службы в органах местного самоуправления.

Поэтому при утечки этой секретной информации страдают интересы службы (а не клиентов, как в случае профессиональной тайны).

В 2003 г. был внесен в думу законопроект «О служебной тайне»

Ответственность за разглашение «служебной тайны» дана в ст.139 части первой ГК РФ “Служебная и коммерческая тайна”:

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки.

Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Законы, защищающие служебную тайну:

1. Закон РФ от 31.07.95 №119-ФЗ “Об основах государственной службы РФ”.
2. Закон РФ от 17.01.92 №2202-1 “О прокуратуре РФ”.
3. Закон РФ от 02.12.90 №395-1 “О банках и банковской деятельности”.
4. Закон РФ от 07 февраля 2011 г. №3 ФЗ “О полиции”.
5. Закон РФ от 12.08.95г. №144-ФЗ “Об оперативно-розыскной деятельности”.
6. Закон РФ от 16.02.95 №15-ФЗ “О связи”.
7. Закон РФ от 29.07.2004г. №98-ФЗ "О коммерческой тайне".
8. Гражданский кодекс РФ от 13.06.96 №63-ФЗ.
9. Таможенный кодекс РФ утв. ВС РФ 18.06.93 №5221-1

Виды служебной тайны:

Аудиторская тайна (всякие результаты аудиторских проверок)

Банковская

Налоговая

Патентная

Следствия

Судопроизводства

32.Правовое регулирование персональной тайны. Основные положения закона РФ «О персональной тайне». Классификация информационных систем ПД.

Основная идея ФЗ № 152 "О персональных данных" в том, что гражданин, являющийся владельцем ПД, сам может определять то, кому он разрешает пользоваться соответствующими данными и каким образом. То есть, если соответствующего разрешения не получено, другое лицо не вправе каким-либо образом обрабатывать ПД, принадлежащие другому субъекту. **Закон устанавливает ряд исключений из этого правила.**

Классификация информационных систем ПД:

категория 1 - ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 - ПД, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением ПД, относящихся к категории 1;

категория 3 - ПД, позволяющие идентифицировать субъекта персональных данных;

категория 4 - обезличенные и (или) общедоступные ПД.

Основные положения закона «О персональной тайне»:

В соответствии с законом существуют следующие виды обработки персональных данных:

-**сбор**;

-**систематизация**;

-**накопление**;

-**хранение**;

-**уточнение** (обновление, изменение);

-**использование** — действия (операции) с ПД, совершаемые оператором в определенных целях;

-**распространение** (в том числе передача) — действия, направленные на передачу ПД определенному кругу лиц;

-**обезличивание** — действия, в результате которых невозможно определить принадлежность ПД конкретному субъекту;

-блокирование — временное прекращение сбора, систематизации, накопления, использования, распространения ПД;

-уничтожение — действия, в результате которых невозможно восстановить содержание ПД в информационной системе или в результате которых уничтожаются материальные носители ПД.

Область применения:

Законом регулируются отношения, связанные с обработкой ПД при использованием 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.

Тоже важная инфа:

Невыполнение требований указанных правовых актов по вопросам обработки ПД, может привести к

►конфликту с государственными органами, осуществляющими контроль и надзор в данной сфере деятельности (Роскомнадзор, ФСБ России, ФСТЭК России),

►привлечении организации и (или) ее руководителя к административной или иным видам ответственности.

Возможны также гражданские иски к организации, принудительное приостановление или прекращение обработки ПД в организации, приостановление действия или аннулирование лицензий.

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

Согласно статье 4 ФЗ № 98, право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона [1]. В действительности над разработкой перечня сведений, составляющих коммерческую тайну, работают сотрудники

юридического отдела, отдела кадров или службы безопасности организации. Наилучшим решением является их совместное участие в разработке перечня. Для этого издается приказ руководителя организации о создании комиссии из 4–5 специалистов основных подразделений и представителей службы безопасности. В такую рабочую группу могут входить сотрудники, которые могут быть ознакомлены как с деятельностью всей организации, так и с работой ее отдельных подразделений.

К коммерческой тайне не могут относиться следующие сведения:

информация о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими бюджетов;

о загрязнении окружающей среды, о степени безопасности жизни граждан;

о количестве работников, о системе оплаты труда, об условиях охраны труда и о показателях производственного травматизма;

о нарушениях законов РФ;

о задолженностях работодателя перед работниками;

о размере и структуре доходов и расходов организации.

Режим коммерческой тайны считается установленным, если обладатель КТ принял меры (в соответствии с законом «О коммерческой тайне»:

-определил **перечень информации**, составляющей КТ, и довел их до сведения работников **под роспись**;

-ограничил свободный доступ к информации, составляющей коммерческую тайну;

-организовал **договорное регулирование отношений** с работниками по вопросам условий передачи и использования информации, составляющей КТ;

-нанес на материальные носители информации, составляющей КТ, и (или) сопроводительные документы **гриф «Коммерческая тайна»**.

-ознакомил **под распись** работника с установленным

на предприятии **режимом** КТ.

Правовые основы защиты информации ограниченного доступа:

В законодательстве **не предусматривается сегодня возможность доступа к профессиональной тайне, со стороны государственных органов** – только в двух случаях: **в отношении адвокатской тайны и тайны исповеди.**

В УК РФ прямо **предусматривается уголовная ответственность лишь в случае разглашения** двух видов профессиональной тайны **– тайны усыновления** (ст. 155 УК РФ) **и тайны связи** (ст. 138 УК РФ).

Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан -наказывается штрафом в размере **до восьмидесяти тысяч рублей** или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо **обязательными работами на срок от ста двадцати до ста восьмидесяти часов**, либо **исправительными работами на срок до одного года. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, - наказывается** штрафом в размере **от ста тысяч до трехсот тысяч рублей.**

Разглашение тайны усыновления (удочерения) вопреки воле усыновителя, совершенное лицом, обязанным хранить факт усыновления (удочерения) как **служебную** или **профессиональную** тайну, либо иным лицом из **корыстных** или иных низменных побуждений, **-наказывается штрафом** в размере **до восьмидесяти тысяч рублей** или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо исправительными работами на срок до одного года, **либо арестом на срок до четырех месяцев**

Лица, незаконными методами получившие информацию, которая составляет **служебную** или коммерческую **тайну**, **обязаны возместить причиненные убытки**.

34.Актуальность защиты коммерческой информации, угрозы и методы защиты, правовая защита.

Коммерческая тайна регулируются Федеральным законом от 29 июля 2004 г. N 98-ФЗ О коммерческой тайне.

В соответствии с этим законом стоит отметить, что право на отнесение той или иной информации к коммерческой тайне принадлежит обладателю информации. Обладатель информации может предпринимать меры, препятствующие получению информации, тем самым защищая её. Информация, составляющая коммерческую тайну считается незаконно полученной, если ее получение осуществлялось с умышленным преодолением предпринятых мер обладателем информации, составляющей коммерческую тайну

К коммерческой тайне не могут относиться следующие сведения:

информация о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими бюджетов;

о загрязнении окружающей среды, о степени безопасности жизни граждан;

о количестве работников, о системе оплаты труда, об условиях охраны труда и о показателях производственного травматизма;

о нарушениях законов РФ;

о задолженностях работодателя перед работниками;

о размере и структуре доходов и расходов организации.

Угрозы КТ:

Внешние угрозы включают три группы субъектов, которые могут быть заинтересованы в получении сведений, составляющих коммерческую тайну:

непосредственные конкуренты, которые действуют на тех же рынках, или компании, которые планируют выйти на те же рынки и осуществляют различные сценарии подрыва положения компании;

субъекты, заинтересованные в переделе долей участия в предприятии, рейдерские группировки, миноритарные акционеры и иные лица, которые могут использовать полученные сведения в борьбе за активы;

субъекты, которые посягают на активы, принадлежащие компании: недвижимость, земельные участки, акции и доли. Получение данных об активах облегчит процесс.

Внутренние угрозы прежде всего связаны с персоналом компании, включая и топ-менеджеров. Сотрудники с доступом к корпоративным информационным системам

могут присвоить сведения, составляющие коммерческую тайну, чтобы продать, использовать в собственных коммерческих проектах или распространить среди неопределенно широкого круга лиц с целью причинить вред компании.

Система защиты должна определить все возможные угрозы и включать механизмы борьбы с конкретными опасностями.

Меры защиты КТ:

Издание приказа о введении режима коммерческой тайны. В документе определяются основные параметры системы защиты и лица, ответственные за организацию защитных мероприятий.

Определение перечня сведений, относящихся к коммерческой тайне.

Разработка системы локальных нормативных актов, которые обеспечат соблюдение режима конфиденциальности и защиту сведений, составляющих коммерческую тайну. Помимо основного документа – положения «О коммерческой тайне» – могут быть разработаны положения о работе со средствами электронно-вычислительной техники и т.д.

Определение круга лиц, у которых есть право работать с материалами, где содержатся сведения, составляющие коммерческую тайну, и уровень допуска.

Разработка трудовых договоров и договоров с контрагентами, которые содержат норму о защите коммерческой тайны.

Включение в договоры с контрагентами условия о конфиденциальности в случаях, когда информация, доверенная контрагенту или его сотрудникам в связи с выполнением условий договора, составляет коммерческую тайну. Контрагентами подобного рода могут быть аудиторские, консалтинговые, оценочные и другие компании. Пункт в договоре должен обязывать в полном объеме компенсировать ущерб, причиненный разглашением тайны.

Функционирование грифов «коммерческая тайна» для защиты конфиденциальной информации и средств идентификации копий документов. Это не защищает документы от копирования в целях передачи информации потенциальным заказчикам, но ограничивает распространение среди широкого круга лиц в открытом доступе.

Особые режимы пользования телекоммуникационным оборудованием, копировальными устройствами, внешней электронной почтой, интернетом.
Строгий контроль за использованием учетных записей.

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.**

   Верхний уровень: документация на уровне руководства.

   Средний уровень: частные политики безопасности, политики использования средств криптозащиты, политики антивирусной защиты, политики мониторинга и управления инцидентами и т.п.

   Нижний уровень: действия по обеспечению ИБ на уровне сетевых сервисов, руководства, инструкции, регламенты, правила администрирования.

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.

Средний уровень: частные политики безопасности, политики использования средств криптозащиты, политики антивирусной защиты, политики мониторинга и управления инцидентами и т.п.

Нижний уровень: действия по обеспечению ИБ на уровне сетевых сервисов, руководства, инструкции, регламенты, правила администрирования.

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

   Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 367 "Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации".

   Цели и задачи проекта ГосСОПКА. Основные положения и нормативные акты, регулирующие деятельность по обнаружению, предупреждению и ликвидации последствий кибератак. Перечень мероприятий для субъектов КИИ. Этапы реализации требований приказа ФСТЭК РФ №239. Требования приказа ФСТЭК РФ №239. Реестр значимых объектов КИИ.

   https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii

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 №620, 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. В свою очередь, организации с критической инфраструктурой (КИИ) должны развернуть у себя центры ГосСОПКА в соответствии с нормативной базой, разработанной ФСБ России.

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 работы — 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

Каждому значимому объекту КИИ РФ присваивается регистрационный номер, состоящий из групп цифр и прописных букв, разделенных косыми чертами, который имеет вид: XXXXXX/X/XX/X

¬ порядковый номер;

¬ федеральный округ, на территории которого находится значимый объект КИИ;

¬ сфера (область) деятельности, в которой функционирует значимый объект КИИ;

¬ тип значимого объекта КИИ

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

   Функции, задачи. Прокомментировать три функциональных уровня (уровень сбора, уровень ядра, уровень управления), каким образом эти уровни реализованы, какие компоненты в каждый уровень входят?

Техническое проектирование является необходимым условием для реализации комплексного подхода к созданию систем обеспечения информационной безопасности. В отсутствии технического проекта возможно лишь реализация фрагментарных мер и механизмов безопасности, за счет которых в современных условиях невозможно решение основных вопросов обеспечения информационной безопасности.

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;

криптографическая подсистема;

инфраструктура открытых ключей;

подсистема защиты от вредоносного ПО;

подсистема фильтрации контента и предотвращения утечки конфиденциальной информации;

подсистема установки обновлений ПО; подсистема администрирования безопасности.

Условно АСУИБ можно разделить на три функциональных уровня: ¬ уровень сбора, ¬ уровень ядра, ¬уровень управления.

Уровень ядра. Здесь происходит сбор, анализ и обнаружение корреляции между событиями безопасности, поступающими от систем обеспечения информационной безопасности и различных компонент ИТ-инфраструктуры. Работа уровня ядра настраивается в соответствии с политикой ИБ, принятой в организации. 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.

Уровень сбора. 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. Уровень управления АСУИБ может иметь различный вид. В самом простом случае это набор организационных мер, организационно-распорядительной документации и те средства визуализации и отчетности, которые предоставляет SIEM-система.

4. **Угрозы информационной безопасности.**

   Определение угрозы, источники угрозы, уязвимость, критичность реализации угрозы, модель угроз.

   Критерии классификации угроз (по аспекту ИБ – CIA, STRIDE, Гексада Паркера, 5A).

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

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

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

Источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Уязвимость (vulnerability) – Любое слабое место в программном обеспечении, которое могло бы использоваться для нарушения целостности системы или содержащейся в ней информации.

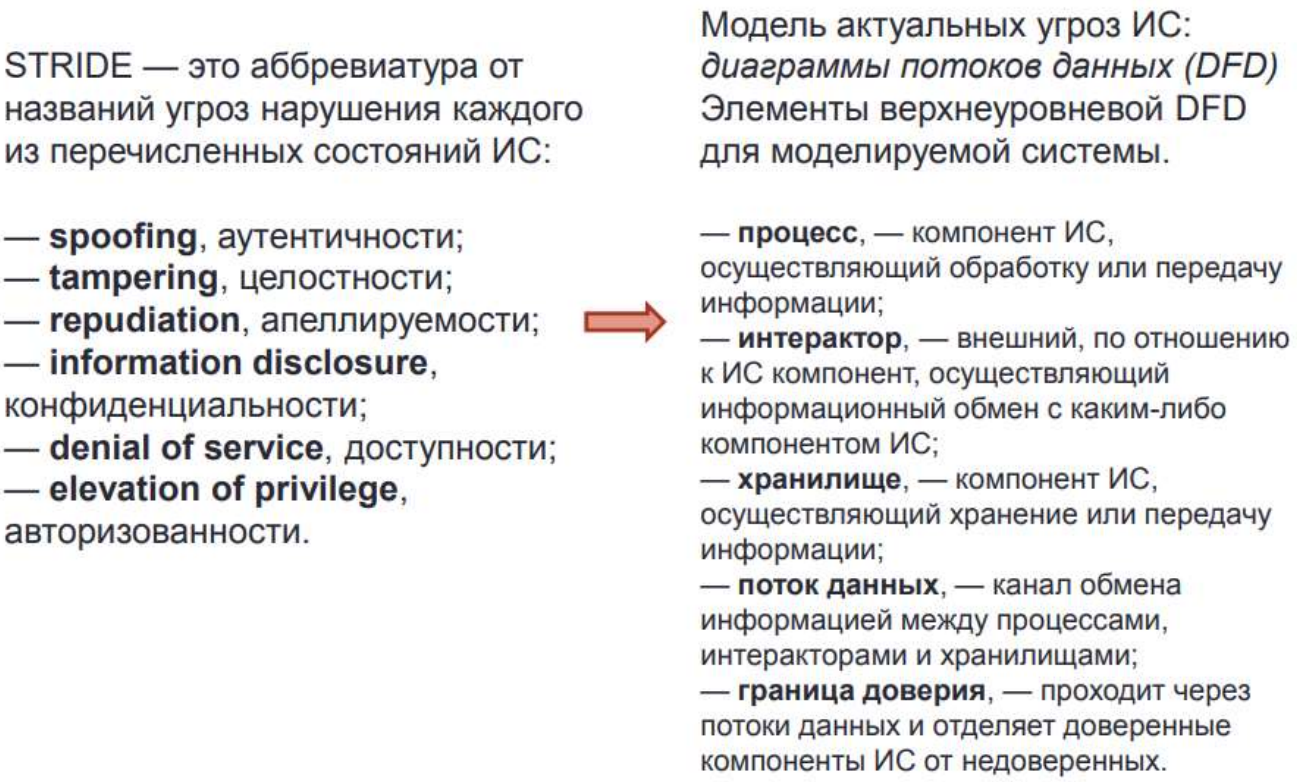
Критичность ресурса (AC) – степень значимости ресурса для информационной системы, т.е. как сильно реализация угроз информационной безопасности на ресурс повлияет на работу информационной системы. Задается в уровнях (количество уровней может быть в диапазоне от 2 до 100) или в деньгах. В зависимости от выбранного режима работы, может состоять из критичности ресурса по конфиденциальности, целостности и доступности (ФСc, ACi, Aci).

Стандартная модель безопасности информации «CIA»:
1.конфиденциальность (confidentiality) - сохранение информации в тайне, невозможность раскрытия информации без согласия заинтересованных сторон;
2.целостность (integrity) - непротиворечивость и правильность информации, защита информации от неавторизованной модификации;
3.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:**
4.подлинность (authenticity) - в применении к пользователю соответствие участника взаимодействия своему имени;
5.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
6.полезность (utility) - удобство доступа; нахождение информации в такой форме, что ее владелец не должен тратить неоправданных усилий.

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

Модель угроз «STRIDE+LM» компонент, используемой Microsoft методологии SDL (Secure Development Lifecycle).
1. Spoofing (аутентификация)
2. Tampering (изменение, целостность)
3. Repudiation (отказ от ответственности)
4. Information Disclosure (утечка данных)
5. Denial of Service (отказ в обслуживании)
6. Elevation of Privilege (захват привилегий, авторизация)
+
7. Lateral Movement (горизонтальное или боковое движение)



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

5. **Стандарт OWASP (Open Web Application Security Project).**

   Рейтинг OWASP Top 10 2021 десяти наиболее опасных рисков информационной безопасности для веб-приложений и мобильных рисков.

   Методика OWASP Risk Rating Methodology, критерии оценки рисков. Рейтинг рисков ИБ веб-приложений: A1-A10. Перечислите их.

   https://owasp.org/www-project-top-ten/

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.

Примеры сценариев атаки

Сценарий № 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 № 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

6. **Протокол автоматизации управления данными безопасности (SCAP).**

   Набор открытых стандартов, определяющих технические спецификации для представления и обмена данными по безопасности. Какие стандарты, языки, отчеты, перечни и системы оценок входят в SCAP? Назовите их.

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 CCE™)
- 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 OVAL™)
- 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/

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

   Оценка цепочки Угрозы-Активы-Уязвимости. Вероятности их реализации. Оценка информационных рисков. Обработка информационных рисков (принятие, уклонение, передача, снижение). Документ «Положение о применимости». Этапы анализа рисков. Внешний и внутренний контекст.

Идентификация активов, классы активов согласно стандарту. Определение ценности активов. Оценка влияния инцидентов на активы.

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]. Составляющими процесса управления рисками являются процедуры своевременного выявления рисков (risk identification), их оценка (risk assessment) и последующая обработка (risk treatment). Методология оценки рисков информационной безопасности предусматривает такие шаги, как: • выявление уязвимостей (организационных и технических); • выявление угроз, направленных на рассматриваемые активы; • определение последствий от реализации угроз; • выявление существующих контролей (контрмер); • определение вероятности реализации угроз.

В качестве мер IT-риска выступают threat (угроза), vulnerability (уязвимость) и ценность актива:

$$Risk=Threat*Vulnerability*Asset$$

Другой вариант (с учетом контмер):

$$Risk=((Vulnerability*Threat)/CounterMeasure)*Asset\_VaR$$

Показатель Value at Risk (VaR) – стоимостная мера риска, выраженная в денежных единицах оценка величины, которую не превысят ожидаемые в течение данного периода времени потери с заданной вероятностью.

* VaR — это величина убытков, которая с вероятностью, равной уровню доверия (например, 99 %), не будет превышена. Следовательно, в 1 % случаев убыток составит величину, большую чем VaR.

Затраты на защиту информационного актива и прочие экономические факторы (объекты или информация) влияют на стоимость актива для организации и мер по его защите. Убыток, реализуемый посредством реализации риска и его негативных последствий, в стандарте расценивается как снижение стоимости
актива.

VaR характеризует наибольший убыток за определённый период времени, который не будет превышен с ожидаемой вероятностью» *[ISO/IEC TR 27016:2014 Information security – Security techniques – Information security management –Organizational economics].*

В свою очередь, размер убытков характеризуется показателем **ALE** (ожидаемый среднегодовой убыток).

ALE = ARO * SLE,

где

ALE (annualized loss expectancy) - ожидаемые потери в год,

ARO (annual rate of occurrence) – частота возникновения инцидента течение года;

SLE (single loss expectancy) – размер потерь в случае одного инцидента.

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

   Методология оценки рисков информационной безопасности, шаги:

   • *выявление угроз, направленных на рассматриваемые активы;*

   • *определение последствий от реализации угроз;*

   • *выявление уязвимостей;*

   • *выявление существующих контролей (контрмер);*

   • *определение вероятности реализации угроз.*

   Формулы для расчета риска: показатель VaR, ALE, ARO, SLE.

Расчет рисков по методике CVSS 3.0 Common Vulnerability Score System. Общая система оценки уязвимостей. Метрики CVSS. Основные пользователи системы. Описание базовых, контекстных, временных метрик. Комментарии, примеры. Формулы расчета риска. Калькулятор. Примеры уязвимостей. Документ МСЭ Т-

REC-X.1521-3.0 (03/2016) СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ. Обмен информацией, касающейся кибербезопасности – Обмен информацией об уязвимости/состоянии. Система оценки общеизвестных уязвимостей 3.0. https://www.first.org/cvss/calculator/3.0 https://nvd.nist.gov/vuln/detail/CVE-2022-22284

Общая система оценки уязвимостей *[Common Vulnerability Scoring System, CVSS]*, версия 2.0 (3.1-текущая) – открытая схема для обмена и оценки уязвимостей ИТ. В этой системе используются группы метрик, а также дается описание базовых метрик *[base metrics]*, вектора уязвимости *[vector]* и оценок уязвимости.

Группы метрик CVSS 3.0:

I. *Базовые метрики:* используются для описания основополагающих сведений об уязвимости — возможности эксплуатации уязвимости и воздействии уязвимости на систему, не изменяются со временем и не зависят от среды.

II. *Временные метрики [temporal]:* при оценке метрики учитывается время, например, опасность уязвимости *[severity of the vulnerability]* снижается с выходом официального обновления безопасности *[official patch]*.

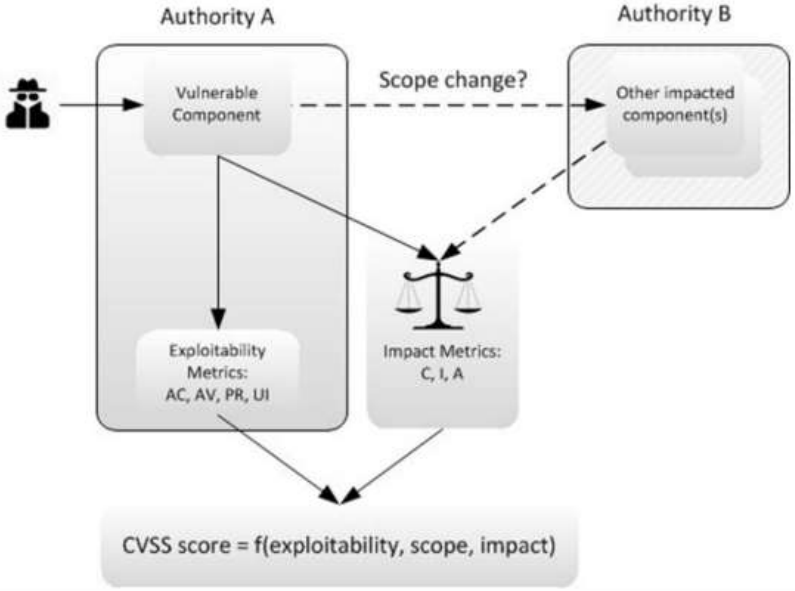
III. *Контекстные метрики [environmental]:* вопросы контекста, среды принимаются во внимание при оценке опасности уязвимости. Например, чем больше систем подвержены *[affected]* уязвимости, тем выше ее опасность.

Компоненты системы, для которых рассчитываются метрики:
уязвимый компонент (vulnerable component) — тот компонент информационной системы, который содержит уязвимость и подвержен эксплуатации;
атакуемый компонент (impacted component) — тот, конфиденциальность, целостность и доступность которого могут пострадать при успешной реализации атаки.
В большинстве случаев уязвимый и атакуемый компоненты совпадают, но есть целые классы уязвимостей, для которых это не так, например:

- выход за пределы песочницы приложения;
- получение доступа к пользовательским данным, сохраненным в браузере, через уязвимость в веб-приложении (XSS);
- выход за пределы гостевой виртуальной машины.

CVSS v 3: **Метрики эксплуатируемости** для **уязвимого компонента**
Метрики воздействия для **уязвимого** и **атакуемого компонента**

Компоненты системы, для которых рассчитываются метрики:
уязвимый компонент (vulnerable component) — тот компонент информационной системы, который содержит уязвимость и подвержен эксплуатации;
атакуемый компонент (impacted component) — тот, конфиденциальность, целостность и доступность которого могут пострадать при успешной реализации атаки.



---

9. **Управление рисками информационной безопасности. Идентификация и оценка технических уязвимостей.**
   Расчет рисков по методике CVSS 3.0 Common Vulnerability Score System. Общая система оценки уязвимостей.
   Метрики CVSS. Основные пользователи системы. Описание базовых, временных и контекстных метрик. Комментарии, примеры. Калькулятор. Разобрать пример уязвимости из базы NVD.

   Документ МСЭ T-REC-X.1521-3.0 (03/2016) СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ. Обмен информацией, касающейся кибербезопасности – Обмен информацией об уязвимости/состоянии. Система оценки общеизвестных уязвимостей 3.1.
   https://www.first.org/cvss/calculator/3.0
   https://nvd.nist.gov/vuln/detail/CVE-2022-22284

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

https://cwe.mitre.org/data/index.html

Документ МСЭ-Т X.1524 (03/2012) СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ. Обмен информацией, касающейся кибербезопасности – Обмен информацией об уязвимости/состоянии. Перечень общеизвестных слабых мест CWE.

CWE List – перечень общеизвестных слабых мест, описание, представление информации. Примеры.

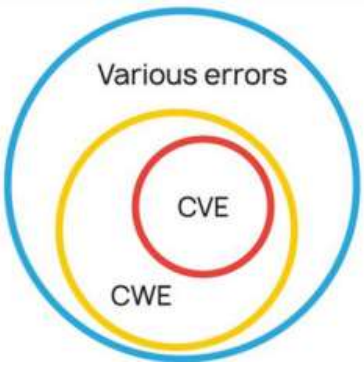
9. Управление рисками информационной безопасности. База Common Weakness Enumeration. Классификация общеизвестных слабых мест CWE.

https://cwe.mitre.org/data/index.html
Документ МСЭ-Т X.1524 (03/2012) СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ. Обмен информацией, касающейся кибербезопасности – Обмен информацией об уязвимости/состоянии. Перечень общеизвестных слабых мест CWE.

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.

Перечень CWE предназначен для того, чтобы охватить причины всех общеизвестных видов уязвимости и незащищенности, связанных со слабыми местами в архитектуре, проектировании, кодировании или развертывании программного обеспечения.

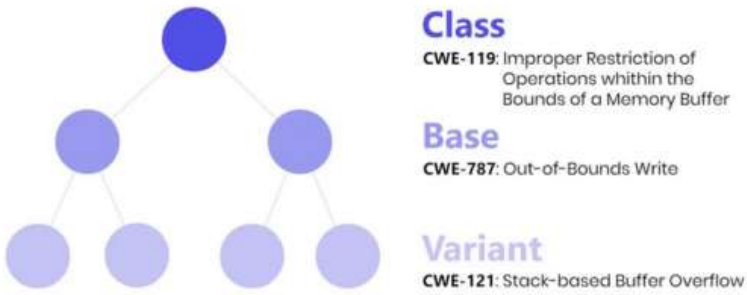
Слабое место (weakness) - дефект или изъян в коде, проектировании, архитектуре или развертывании программного обеспечения, способный в определенный момент стать уязвимостью или приводить к возникновению других уязвимостей.



Ошибки в программном обеспечении, которые могут быть непосредственно использованы злоумышленником для реализации угроз безопасности называют **уязвимостями**.
Ошибки, которые могут привести к возникновению уязвимостей – **недостатками безопасности**.

Для классификации недостатков используется многоуровневая структура, которая описывает древовидное устройство CWE: конечные недостатки объединяются в типы, типы – в категории, категории – в представления. Каждое представление – особый способ классификации записей CWE, предназначенный для упрощения решения конкретной задачи.

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



Type (тип) – это абстракция (метка) слабого места. Тип обозначается одним из символов:

V (variant) - Вариант - слабость, которая связана с определенным типом продукта, обычно с использованием определенного языка или технологии. Более конкретная, чем базовая слабость. Слабые стороны уровня варианта обычно описывают проблемы с точки зрения 3-5 следующих параметров: поведение, свойство, технология, язык и ресурс;
C (class) - Класс - это слабость, которая описывается очень абстрактно, как правило, независимо от какого-либо конкретного языка или технологии. Более конкретный, чем Pillar, но более общий, чем База. Слабые стороны уровня класса обычно описывают проблемы в терминах 1 или 2 следующих измерений: поведение, свойство и ресурс;
B (Base) - База - слабость, которая по-прежнему в основном не зависит от ресурса или технологии, но обладает достаточными деталями, чтобы предоставить конкретные методы обнаружения и предотвращения. Слабые стороны базового уровня обычно описывают проблемы в терминах 2 или 3 следующих параметров: поведение, свойство, технология, язык и ресурс;
Chain – Цепочка - сложный элемент, представляющий собой последовательность двух или более отдельных слабых мест, которые могут быть тесно связаны между собой в рамках программного обеспечения. Одна слабость, X, может непосредственно создать условия, необходимые для того, чтобы другая слабость, Y, вошла в уязвимое состояние. Когда это происходит, CWE обращается к X как к "первичному" Y, а Y является "результирующим" от X. цепочки могут включать более двух слабых мест, и в некоторых случаях они могут иметь древовидную структуру.
Composite – Композит - сложный элемент, состоящий из двух или более различных слабых мест, в котором все слабые места должны присутствовать одновременно, чтобы возникла потенциальная уязвимость. Устранение любого из недостатков устраняет или резко снижает риск. Одна слабость, X, может быть "разбита" на составляющие слабости Y и Z. бывают случаи, когда одна слабость может не быть существенной для композита, но изменяет природу композита, когда он становится уязвимым.

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

https://cwe.mitre.org/cwss/cwss_v1.0.1.html

Документ МСЭ-Т X.1525 СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ. Обмен информацией, касающейся кибербезопасности – Обмен информацией об уязвимости/состоянии. Система оценки общеизвестных слабых мест (CWSS). Открытая структура представления информации о характеристиках и воздействиях слабых мест информационно-коммуникационных технологий (ИКТ) в ходе разработки возможностей программного обеспечения.

Группы метрик:

Base Finding metric group (Базовые), Attack Surface metric group (Поверхность атаки), Environmental metric group (Контекстные). Примеры метрик.

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

https://cwe.mitre.org/data/index.html
https://cwe.mitre.org/cwss/cwss_v1.0.1.html

Документ МСЭ-Т X.1525 СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ. Обмен информацией, касающейся кибербезопасности – Обмен информацией об уязвимости/состоянии. Система оценки общеизвестных слабых мест (CWSS). Открытая структура представления информации о характеристиках и воздействиях слабых мест информационно-коммуникационных технологий (ИКТ) в ходе разработки возможностей программного обеспечения.

Каждая группа содержит несколько метрик- так же обозначаемых как факторы (factors) - которые применяются для вычисления оценки CWSS score (CWSS score, between 0 and 100) для каждого слабого места.

- Группа показателей базовых: охватывает внутренние риски, присущие слабому месту, доверие к точности результатов поиска, а также действенность средств контроля.
- Группа показателей области атаки: барьеры, которые должен преодолеть злоумышленник, для того чтобы эксплуатировать слабое место.
- Группа показателей среды: характеристики слабого места, присущие конкретной среде или операционному контексту.

Подробное описание метрик и примеры есть в документе МСЭ-Т X.1525.

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

https://cwe.mitre.org/top25/index.html

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

https://cwe.mitre.org/top25/index.html

Rank	ID	Name	Score	KEV Count (CVEs)	Rank Change vs. 2021
1	CWE-787	Out-of-bounds Write	64.20	62	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97	2	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11	7	+3 ▲
4	CWE-20	Improper Input Validation	20.63	20	0
5	CWE-125	Out-of-bounds Read	17.67	1	-2 ▼
6	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17.53	32	-1 ▼
7	CWE-416	Use After Free	15.50	28	0
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.08	19	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.53	1	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	9.56	6	0
11	CWE-476	NULL Pointer Dereference	7.15	0	+4 ▲
12	CWE-502	Deserialization of Untrusted Data	6.68	7	+1 ▲
13	CWE-190	Integer Overflow or Wraparound	6.53	2	-1 ▼
14	CWE-287	Improper Authentication	6.35	4	0
15	CWE-798	Use of Hard-coded Credentials	5.66	0	+1 ▲
16	CWE-862	Missing Authorization	5.53	1	+2 ▲
17	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	5.42	5	+8 ▲
18	CWE-306	Missing Authentication for Critical Function	5.15	6	-7 ▼
19	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.85	6	-2 ▼
20	CWE-276	Incorrect Default Permissions	4.84	0	-1 ▼
21	CWE-918	Server-Side Request Forgery (SSRF)	4.27	8	+3 ▲
22	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.57	6	+11 ▲
23	CWE-400	Uncontrolled Resource Consumption	3.56	2	+4 ▲
24	CWE-611	Improper Restriction of XML External Entity Reference	3.38	0	-1 ▼
25	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.32	4	+3 ▲

13. Управление инцидентами информационной безопасности.

SOC: создание ситуационного центра ИБ. Центр оперативного управления информационной безопасностью. Цели и задачи группы реагирования (incident response), управление событиями ИБ.

SIM (Security information management) — управление информационной безопасностью, и SEM (Security event management) — управление событиями безопасности.

SIEM (Security information and event management) системы – задачи и функционал.

14. Управление инцидентами информационной безопасности.

Системы поведенческого анализа - User and Entity Behavioral Analytics (UBA).

User [and Entity] Behavioral Analytics (UBA), как 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. Цели и задачи таких систем. Основные возможности.

15. Управление инцидентами информационной безопасности.

APT (англ. advanced persistent threat — «развитая устойчивая угроза»; целевая кибератака).

Цели и характерные особенности. Типовой сценарий APT-атаки и этапы.

The Cyber Kill Chain. *Киллчейн, как последовательные стадии, которые проходит злоумышленник для успешной реализации атаки. Основные этапы и их характеристики. Примеры.*

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

Характерные признаки (observables) и индикаторы компрометации (indicators of compromise, IOC).

Что представляют собой показатели компрометации IoC, и показатели атаки IoA? Приведите примеры типичных IoC и IoA. Прокомментируйте рисунок ниже.

IoC (Indicator of Compromise)
Показатели компрометации

APT (Advanced Persistent Threat) кампания или атака - «развитая устойчивая угроза» или «сложная постоянная угроза», подразумевающая многоэтапный сценарий атаки. Типичный отчет об APT-кампании содержит следующую информацию:

- Жертвы атаки и цели, которые преследуют злоумышленники;
- Перечень узлов (IP-адреса) жертв;
- Текущая активность вредоносных компонентов и/или киберпреступных групп;
- Детальное описание инструментов и вредоносных компонент, которые используют злоумышленники;
- Описания инфраструктуры командных центров (C&C);
- **Показатели компрометации и атаки.**

IoC (Indicator of Compromise) Показатели компрометации

APT (Advanced Persistent Threat) кампания или атака - «развитая устойчивая угроза» или «сложная постоянная угроза», подразумевающая многоэтапный сценарий атаки. Этапы APT:

- ✓ Пассивный сбор информации (идентификация и отбор целей из открытых источников).
- ✓ Первичное заражение (заманивание на фишинговые сайты, рассылка инфицированных документов).
- ✓ Доставка боевой нагрузки (drive-by-загрузки, использование уязвимостей в браузере и его плагинах).
- ✓ Активная фаза (повышение привилегий и обход защитных систем с целью получения дополнительных данных о системе и закрепления в ней основных вредоносных компонентов).
- ✓ Получение удаленного контроля (внедрение бэкдоров, кейлоггеров и установка обратных шеллов).
- ✓ Связь с управляющими серверами в ожидании дальнейших команд (обход файрволов, использование для передачи команд различных мессенджеров, клиентов соцсетей и популярных сетевых API).
- ✓ Достижение конечной цели (кража данных, выполнение незаконных финансовых транзакций, формирование ботнета, перехват контроля над АСУ ТП и так далее).

IoC (Indicator of Compromise) Показатели компрометации

IOC (indicator of compromise) – перечень данных об угрозах (например, строки, описывающие путь к файлам или ключи реестра), который дает возможность, используя автоматизированный анализ программными средствами, выявить наличие угрозы в инфраструктуре.

Существуют различные форматы представления этих данных, например, OpenIOC.
Эти форматы позволяют импортировать данные в то или иное защитное решение для последующей работы с **индикаторами**.

Администратор может осуществить интеграцию IOC, взятых из отчетов, в различные защитные решения:

Средства защиты класса «Endpoint Security»:

- SIEM
- IDS/IPS
- HIDS/HIPS
- инструменты для расследования инцидентов

IoC (Indicator of Compromise)
Показатели компрометации

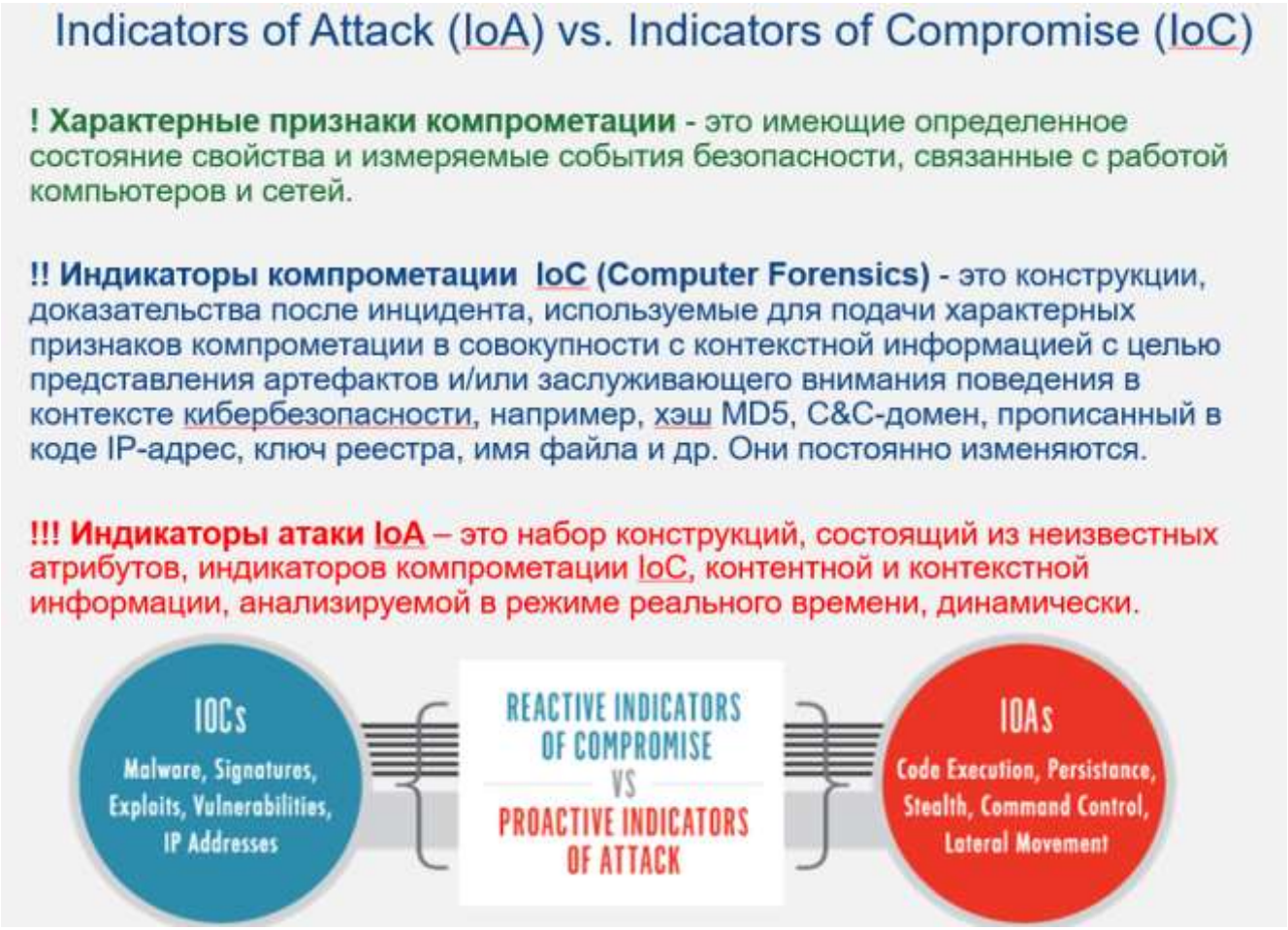
Характерные признаки **(observables)** и индикаторы **компрометации (indicators of compromise, IOC)** - формат, описанный в статье MITRE от 2012 года, *A structured language for cyber threat intelligence, STIX.*

! **Indicator of compromise (IOC)** - in computer forensics is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion.

!! **Typical IOCs** are virus signatures and IP addresses, MD5 hashes of malware files or URLs or domain names of botnet command and control servers.

After IOCs have been identified in a process of incident response and computer forensics, they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software.

https://oasis-open.github.io/cti-documentation/stix/intro



10 Indicators of Attack (IoA)

1) Внутренние узлы с плохими направлениями

Внутренние узлы, осуществляющие связь с заведомо плохими пунктами назначения или с иностранными государствами, где вы не ведете бизнес.

2) Внутренние узлы с нестандартными портами

Внутренние узлы, общающиеся с внешними узлами с использованием нестандартных портов или несоответствия протокола/порта, например, отправка командной оболочки (SSH), а не HTTP, трафик HTTPS через порт 80,443, веб-порт по умолчанию.

3) Публичные серверы/ДМЗ к внутренним хостам

Публичные серверы или хосты демилитаризованной зоны (DMZ) общаются с внутренними хостами. Это позволяет переходить из внешней зоны во внутреннюю и обратно, обеспечивая утечку данных и удаленный доступ к таким ресурсам, как RDP (Remote Desktop Protocol), Radmin, SSH.

4) Обнаружение вредоносного ПО в нерабочее время

Сигналы тревоги, возникающие в нестандартные рабочие часы (ночью или в выходные), могут свидетельствовать о наличии взломанного узла.

5) Сканирование сети внутренними узлами

Сканирование сети внутренними узлами, взаимодействующими с несколькими узлами за короткий промежуток времени, что может выявить атакующего, перемещающегося в сети в боковом направлении.

6) Множественные тревожные события с одного хоста

Несколько тревожных событий с одного узла или дублирование событий на нескольких машинах в одной подсети в течение 24 часов, например, повторяющиеся сбои аутентификации.

7) Система повторно заражена вредоносным ПО

*После очистки зараженного узла система повторно заражается вредоносным ПО в течение 5-10 минут, повторные повторные заражения сигнализируют о наличии руткита или устойчивой компрометации. Этот инцидент может быть обнаружен в результате событий Endpoint Security Protection или Anti-*Virus.

8. Многократный вход в систему из разных регионов

Учетная запись пользователя пытается войти на несколько ресурсов в течение нескольких минут из/в разные регионы. Это признак того, что учетные данные пользователя были украдены или что пользователь замышляет недоброе.

9. Внутренние узлы используют много SMTP

Необходимо следить за такими протоколами электронной почты, как SMTP (Simple Mail Transfer Protocol), POP3 или IMAP4. Некоторые вредоносные программы используют эти порты для отправки информации на подозрительный или хакерский сервер.

10. Внутренние узлы могут запрашивать внешний/внутренний DNS

Многие организации имеют внутренние DNS-серверы для кэширования записей и предоставления услуг DNS внутренним узлам. В конфигурации DHCP первичный DNS-сервер определяется как внутренний DNS-сервер. Если вы обнаружили, что некоторые внутренние узлы запрашивают внешний DNS, например 8.8.8.8, 8.8.4.4 (Google DNS), попробуйте проверить вредоносное ПО на этих клиентах.

17. Управление инцидентами информационной безопасности. 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. Формат JSON для описания угроз, визуализация представления в виде графа. Приведите пример в формате JSON, визуализируйте свой пример.

Архитектура STIX 2.1.

https://oasis-open.github.io/cti-documentation/stix/examples

https://oasis-open.github.io/cti-stix-visualization/

https://oasis-open.github.io/cti-documentation/resources#stix-21-specification

https://github.com/oasis-open/cti-stix2-json-schemas/tree/master/examples

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

Главным элементом платформы Threat Intelligence являются потоки данных, представленные в виде индикаторов компрометации (Indicators of Compromise, IoC).

Они представляют собой признаки, по которым можно обнаружить угрозу безопасности: IP- и URL-адреса, связанные с вредоносной активностью, хеш-суммы вредоносных файлов и т.д.

Последовательность индикаторов компрометации из одного источника принято называть «фидом» (от англ. feed — «подача материала, питание»). Threat Intelligence можно классифицировать следующим образом: по способу получения (например, из открытых источников или путём обмена информацией между специалистами), по типу данных (фиды, представленные в виде хешей вредоносных файлов, DDoS-фиды, C&C-фиды, отчёты о деятельности APT-группировок и др.), а также по влиянию на уровень принятия решений (тактические, технические и стратегические). Далее представить и описать пирамиду индикаторов компрометации в зависимости от сложности получения данных:

19. Анализ данных из открытых источников OSINT. Цели и задачи. OSINT в сфере информационной безопасности. Анализируемые данные. *Пассивные и активные методы OSINT. Автоматизированные инструменты: Shodan, Metagoofil, Maltego, WHOIS.*

Набор запросов для выявления ошибок в безопасности ресурсов Google Dorks.

Примеры. Операторы Google.

https://www.exploit-db.com/google-hacking-database

18. Анализ данных из открытых источников OSINT. Цели и задачи. Методы OSINT.

Активные

Такие методы подразумевают непосредственное влияние аналитика на исследуемый объект, использование специализированных средств получения данных или совершение действий, требующих определенных усилий, например:

- 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.

18. Анализ данных из открытых источников OSINT. Цели и задачи. Методы OSINT.

Все методы и инструменты, используемые для анализа данных из открытых источников, можно разделить на две категории.

Пассивные

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 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.

18. Анализ данных из открытых источников OSINT. Цели и задачи. OSINT в сфере информационной безопасности.

С развитием интернета фокус внимания аналитиков сместился в киберпространство как один из главных источников информации. Здесь полезными данными могут являться:

- регистрационные сведения о сертификате или домене сайта;
- открытые персональные данные пользователей (username, адреса электронной почты, номера телефонов);
- пользовательская активность в социальных сетях (посты, комментарии и т.д.);
- пользовательские запросы в поисковых системах;
- HTML-код сайта;
- публичные текстовые, графические, аудио-, видеофайлы и их метаданные (например, дата, время и место создания, использованное устройство);
- геолокационные данные и другие виды информации.

** Ко многим данным можно получить доступ через открытый интернет с помощью ресурсов, индексируемых поисковыми системами. Однако и источники из «глубинной Сети», к которым у обычных пользователей нет доступа из-за необходимости платить за них, тоже попадают под определение open source. Иными словами, OSINT работает со всеми данными, которые не являются конфиденциальными, не составляют коммерческую или государственную тайну.*

18. Анализ данных из открытых источников OSINT. Цели и задачи. OSINT в сфере информационной безопасности.

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.

** Сбор и анализ информации, находящейся в общественном достоянии, не противоречат нормам международного законодательства, а также законам большинства государств, хотя некоторые источники и способы их исследования могут находиться на грани законности.*

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

Приведите этапы и примеры инструментов сбора, анализа, выявления доказательств.

Например, сбор цифровых доказательств в соответствии с Федеральным законом от 31.05.2001 г. № 73-ФЗ "О государственной судебно-экспертной деятельности в Российской Федерации". Сохранность информации и данных. Источники криминалистически значимой компьютерной информации. Документация накопителей и аппаратной конфигурации систем, Защита от записи, Логирование действий.

Приведите примеры программных блокираторов записи, аппаратных криминалистических копировальщиков с блокировкой записи.

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

Прокомментируйте следующие виды данных:

–данные в состоянии изменения;

–данные, содержащиеся в активной физической памяти;

–данные, которые существуют в транзите;

–системные данные, которые теряются при потере мощности, отключении ПК, холодной перезагрузке.

Live Forensics лучшими практиками являются:

– Использование криминалистического ПО, способного производить побитовое чтение данных через локальную сеть и сохранять данные уже на защищенной системе (например, ПО, которое использует протокол ISCSI, обеспечивающий доступ на уровне блоков к устройствам хранения путем переноса команд SCSI через сеть TCP/IP).

– Использование аппаратного обеспечения для создания чистого дампа памяти через прямой доступ к памяти DMA в сочетании с программным подходом (может быть использовано для сравнительного анализа).

Правило волатильности: «RFC 3227: Рекомендации по сбору и архивированию доказательств»

Порядок для типичной системы (RFC 3227):

–регистры

–оперативная память, кэши, таблица маршрутизации, таблица процессов, статистика ядра

–временные файловые системы

–диск

–физическая конфигурация, сетевая топология

–архивы и файлы

Общее правило: при сборе доказательств вы должны перейти от более к менее волатильному.