ЧАСТЬ 1. НЕКРАСОВ

1. Нормативно-правовое регулирование общественных отношений

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

В основе информационного права правовое регулирование общественных отношений, возникающих в процессе поиска, получения, передачи, производства и распространения информации, а также связанных с ними отношений.

Нормативно-правовое регулирование **осуществляется на основе** созданных уполномоченными субъектами нормативно-правовых актов, законов и других формальных источников права

Предмет правового регулирования — это совокупность общественных отношений, на которые направлено воздействие правовых средств и методов.

Нормативные правовые акты классифицируются по:

1) Юридической силе

1. Законы
2. Подзаконные акты

2) Субъектам, их задающими

1. Акты законодательной власти (законы)
2. Акты исполнительной власти (подзаконные акты)
3. Акты судебной власти (юрисдикционные акты общего характера)

Законы принимаются высшими законодательными органами (Федеральное собрание – ГосДума и Совет Федерации), их принятие включает внесение законопроекта в законодательный орган, его обсуждения, принятие и публикация после подписания Президентом, вступают в силу после 10 дней опубликования, не подлежат контролю или утверждению другого органа государства (могу быть отменены только законодательной властью).

Подзаконные нормативно-правовые акты подразделяются на:

1) **Указы президента**. Они обладают высшей юридической силой и издаются на основе и в развитие законов (вступают в силу по истечении 7 дней после их опубликования).

2) **Постановления правительства**. Принимаются в контексте с указами президента (вступают в силу по истечении 7 дней после их опубликования).

3) **Местные акты**. Акты органов законодательной и исполнительной власти на местах. Действие этих актов ограничено подвластной им территорией.

4) **Ведомственные** (приказы, инструкции). Акты общего действия, распространяются лишь на ограниченную сферу общественных отношений (таможенные, банковские, транспортные, государственно-кредитные и другие).

5) **Внутриорганизационные**. Издаются различными организациями для регламентации своих внутренних вопросов и распространяются на членов этих организаций

Иерархия (от главных к низшим (сверху вниз, слева направо)):

1) Конституция, Федеральные конституционные законы РФ, Федеральные законы РФ, Указы и распоряжения Президента РФ, Законодательные акты субъектов РФ

2) Постановления и распоряжения Правительства РФ, Нормативные правовые акты высших органов исполнительной власти субъектов РФ

3) Нормативные правовые акты федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ

4) Правовые акты органов местного самоуправления

Юридическая ответственность подразделяется по отраслевому признаку:

1) **Уголовная ответственность** наступает за совершение преступлений и устанавливается только уголовным законом.

2) **Административно-правовая ответственность** наступает за совершение административных проступков. Меры административного принуждения – предупреждение, штраф, лишение специального права (на ношение оружия, управление транспортным средством и т.д.), административный арест.

3) **Гражданско-правовая ответственность** наступает за нарушения договорных обязательств имущественного характера или за причинение имущественного внедоговорного вреда. (Возмещение убытков, выплата неустойки).

4) **Дисциплинарная ответственность** возникает вследствие совершения дисциплинарных проступков. Меры дисциплинарной ответственности – выговор, строгий выговор, отстранение от занимаемой должности и т.п.

5) **Материальная ответственность** рабочих и служащих за ущерб, нанесенный предприятию, учреждению. Размер возмещаемого ущерба определяется в процентах к заработной плате (1/3, 2/3 месячного заработка).

2. Система и строение права

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

Вертикальное (от высшего к низшему):

Отрасль (охватывает сферу общественных отношений – в имущественных гражданское право, в управленческих –административное), подотрасль (охватывает область общественных отношений – в гражданском праве есть подотрасли авторское и наследственное право), институт (охватывает вид общественных отношений –в трудовом праве институт трудового договора), сабинститут (охватывает разновидность общественных отношений – сабинститут преступлений против жизни, против здоровья), норма (это обязательное правило поведения, охраняемое силой государственного принуждения), правовое предписание (это часть нормы права, логически завершенная и обособленная).

Горизонтальное строение права показывает все составляющие его отрасли. Выделяют **Регулятивные отрасли** (устанавливают права и обязанности участников правоотношений):

Конституционное право (основы государственного и общественного строя страны по конституции), административное право (общественные отношения, возникающие в процессе исполнительно-распорядительной деятельности органов государства), гражданское право (различные имущественные отношения по ГК), финансовое право (доходы, расходы по ФЗ о госбюджете), банковское право, предпринимательское право, трудовое право, природоресурсное право, информационное право (общественных отношений, связанных с информацией, защитой информации, защитой прав собственников информационных ресурсов, формирования различных институтов тайн).

Охранительные отрасли права:

Уголовное право (устанавливает общественно опасные деяния и наказание по УК), уголовно-процессуальное право (определяет порядок проведения

предварительного следствия, дознания, порядок ведения судебного разбирательства по УПК), - уголовно-исполнительное право (исполнение мер наказания по УИК), гражданско-процессуальное право (порядок рассмотрения споров с гражданином по ГПК), арбитражно-процессуальное право (порядок рассмотрения гражданско-правовых споров между юридическими лицами по АПК).

Так же есть **Международное право** – система юридических принципов и норм, регулирующих отношения между государствами. Делится на Публичное (регулирующая отношения между государствами, созданными ими международными организациями), Частное (регулируют гражданско-правовые, трудовые и иные отношения, осложнённые иностранным элементом), Национальное (форма международного права, при которой государства идут на сознательное ограничение некоторых своих прав и делегирование некоторых полномочий наднациональным органам)

3. Структура информационного законодательства

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

Систему информационного законодательства образуют различные законы и нормативные правовые акты, посвященные прямому или опосредованному регулированию отношений, объектом которых является информация, производные от нее продукты и связанная с ними деятельность.

Предмет правового регулирования в информационной сфере:

– создание и распространение информации;

– формирование информационных ресурсов;

– реализация права на поиск, получение, передачу и потребление информации;

– создание и применение информационных систем и технологий;

– создание и применение средств информационной безопасности

Формирование законодательства в области информационного права в России началось, в основном, со времени появления «Концепции правовой информатизации России», утвержденной Указом Президента РФ от 28.06.93 г. № 966. В основе информационного законодательства находится свобода информации и запретительный принцип права

Структура информационного законодательства:

1) Конституция РФ (конституционные информационно-правовые нормы), ГК, УК, ТК

Международные и российские основополагающие документы:

2) Окинавская Хартия глобального информационного общества от 22 июля 2000 г.

3) Доктрина информационной безопасности РФ от 9 сентября 2000 г.

Нормативно-правовые акты:

4) ФЗ «Об информации, информационных технологиях и о защите информации», «Об электронной подписи», «О коммерческой тайне», «О персональных данных», «О государственной тайне», «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»

Закон «Об информации, информационных технологиях и о защите информации» установил следующие принципы правового регулирования отношений, в информационной сфере (ст. 3):

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

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации;

4) обеспечение безопасности Российской Федерации при создании и эксплуатации информационных систем;

5) достоверность информации и своевременность ее предоставления;

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

7) недопустимость преимуществ применения одних информационных технологий перед другими, кроме государственных информационных систем установленных в соответствии с федеральными законами.

4. Основные определения в области информационного права

Основной нормативно-правовой документ в сфере информационного права Закон РФ “Об информации, информационных технологиях и о защите информации” от 27.07.2006 г. № 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 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

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)

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;

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети

Также обладатель информации, доступ к информации, предоставление, распространение информации, документированная информация, электронный документ, оператор информационной системы

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

5. Права обладателя и режимы доступа к информации

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.

Информация (в зависимости от порядка ее распространения) подразделяется на: свободно распространяемую, предоставляемую по соглашению, распр. в соотв. с ФЗ, запрещённой для распр. в РФ

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 (по ФЗ “Об информации, информационных технологиях и о защите информации” и Указу Пр. РФ “Об утверждении перечня сведений конфиденциального характера”):

Режим доступа: Свободный Вид режима: Общественное достояние (Состав: научные открытия, рукописи) Вид режима: Массовая информация (Состав: СМИ, публикации) Вид режима: Исключительные права (Состав: Интеллектуальная деятельность)

Режим доступа: Ограниченный доступ Вид режима: Конфиденциальность (Состав: ком, служебная тайна, персон.данные, тайна следствия и судопроизводства) Вид режима: Гос тайна (Состав: Секретно, совершенно секретно, особой важности)

6. Сведения, составляющие государственную тайну.

Государственная тайна (ГТ) – защищаемые государством сведения в области его **военной**, **внешнеполитической**, **экономической**, **разведывательной**, **контрразведывательной** и **оперативно-розыскной** деятельности, распространение которых может нанести ущерб безопасности РФ.

Система защиты государственных секретов основывается на Законе РФ «О государственной тайне» от 21.07.1993 г. № 5485-1. Закон регулирует отношения, связанные с отнесением сведений к ГТ, их рассекречиванием и защитой в интересах безопасности РФ.

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.

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

Порядок засекречивания сведений, составляющих ГТ, основан на трех принципах: **законности**, **обоснованности** и **своевременности**.

Обоснованность отнесения сведений к ГТ и их засекречивание заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.

Срок засекречивания сведений, составляющих ГТ, не должен превышать 30 лет.

7. Ответственность за разглашение государственной тайны.

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**. Уголовно-правовая ответственность за разглашение информации, содержащей ГТ, определяется Уголовным кодексом РФ – **ст. 275** (Гос. измена), **276** (Шпионаж), **283** (Разглашение ГТ), **284** (Утрата документов, содержащих ГТ).

При установлении нарушений норм защиты информации используется понятие «утраты документа» – выход документов из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы стали или могли стать достоянием посторонних лиц.

8. Сведения, составляющие коммерческую тайну.

К коммерческой тайне (КТ) относят следующие три группы сведений:

Деловая информация (о сферах деятельности):

– финансовые сведения;

– данные о себестоимости продукции и услуг;

– деловые планы и планы производства и развития;

– информация о маркетинге;

– соглашения, предложения, контракты;

– организационные схемы.

Техническая информация:

– научно-исследовательские проекты;

– конструкторская документация на продукцию;

– заявки на патенты;

– дизайн, передовые технологии и оборудование;

– программное обеспечение ЭВМ и информационный процесс (Информационный процесс – процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.);

– химические формулы.

Информация о клиентах и конкурентах:

На каждого клиента фирмы накапливается информация, где отражаются его привычки, характерные черты поведения, интересы в личной жизни, о представляемых ему фирмой привилегиях и т. п.

Все что связано с КТ содержится в: **Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.06.2006 г. № 149-ФЗ** и **Закон РФ «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ**

Виды разведок:

6. Конкурентная разведка – это сбор и обработка информации законными способами. Четыре вида сбора информации:

– сбор данных о партнерах и клиентах для предотвращения мошенничеств с их стороны;

– информация о потенциальных партнерах и сотрудниках;

– выполнение услуг охраны и сыска;

– сбор информации маркетингового характера.

Методы: наблюдение, отчеты торговых работников, поиск информации в открытых базах данных, анализ годовых отчетов предприятий, обратный инжиниринг.

7. Промышленный шпионаж – незаконный сбор сведений, составляющих коммерческую тайну, незаконное использование секретной информации лицом или предприятием, не уполномоченным на то ее владельцем.

9. Защита коммерческой тайны.

Отличие коммерческой тайны от государственной:

– Сведения, составляющие ГТ, установлены соответствующим перечнем, а КТ этим перечнем не определена и определяется руководителем предприятия.

– ГТ охраняется силой государства в лице соответствующих органов, а коммерческая информация – службой безопасности предприятия.

По аналогии с ГТ коммерческая информация может быть ранжирована по степени ее важности для предприятия с тем, **чтобы регулировать ее распространение** среди работающих на предприятии, указывать пользователей этой информации, уровень ее защиты и т. д.

Закон «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ регулирует отношения, связанные с отнесением информации к КТ, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестной конкуренции, а также определяет сведения, которые не могут составлять КТ.

Степени секретности КТ: КТ – строго конфиденциально (КТ-СК); КТ – конфиденциально (КТ-К); коммерческая тайна (КТ); для внутреннего использования (ДВИ).

Режим КТ – правовые, организационные, технические и иные меры по охране ее конфиденциальности. Законом о КТ (ФЗ-98) установлены требования, предъявляемые к режиму коммерческой тайны. В рамках режима КТ на предприятии вводятся система закрытого делопроизводства.

В случае **нарушения конфиденциальности** информации должностными лицами органов государственной власти эти лица несут **ответственность в соответствии со статьей 14 (ФЗ-98)**: дисциплинарную, гражданско-правовую, административную или уголовную. Также ответственность за разглашение КТ, дана в **УК РФ ст. 183** (Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну).

10. Правовое регулирование отношений по защите коммерческой тайны на предприятии.

В соответствии с установленными законом о КТ, на **предприятии используются правовые нормы внутрифирменных документов для регулирования правовых отношений по защите КТ**. Такими документами являются:

– Устав предприятия;

– Коллективный договор предприятия;

– Трудовые и гражданско-правовые договоры;

– Правила внутреннего трудового распорядка рабочих и служащих предприятия;

– 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 и предприятие обязано обеспечить сохранность КТ.

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 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.

5. Ввести в текст трудового договора требования по защите КТ.

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.

11. Защита коммерческой информации в договорной документации.

Защита коммерческих секретов основывается на внутрифирменных нормативных документах **трудовой договор** (контракт) и **должностные инструкции**.

Трудовой договор – это соглашение между работодателем и работником, в котором определены права и взаимные обязанности сторон.

Должностная инструкция – это внутренний организационно-распорядительный документ, содержащий перечень обязанностей работника, а также его прав и ответственности.

В трудовом договоре различают **основные** (законодательно определенные) и **дополнительные** условия. **Вопросы ЗИ** в трудовом договоре **в виде доп. условий**.

Неразглашение КТ – это обязанность работника, включённая в трудовой договор и др. договоры:

1. **Договор поручительства**: поручитель обязуется отвечать перед кредитором за исполнение обязательства другого лица.

2. **Договор коммерческого представительства**: коммерческий представитель представляет интересы предпринимателей. Действует от их имени.

3. **Агентский договор**: агент обязуется за вознаграждение совершать действия от своего имени, но по поручению другой стороны (принципала).

4. **Договор поручения**: одна сторона (поверенный) обязуется совершить от имени и другой (доверителя) юридические действия. Полномочия поверенного оформляются доверенностью.

5. **Договор о рекламных услугах**.

В этих документах включаются обязательства:

– не разглашать КТ организации 3 лицам;

– сохранять КТ деловых партнеров;

– извещать СБ о попытках получить закрытую информацию;

– предупреждение работника о наступлении гражданской, административной или уголовной ответственности в случае нарушения обязательств.

Обязанности по сохранению КТ возлагаются и на руководителя. В контракт с руководителем **вводятся положения**: 1. – его обязательство не использовать КТ в ущерб организации; – его персональная ответственность за сохранность КТ; – ответственность за последствия нарушений защиты КТ.

Защита прав обладателя КТ по ГК РФ: возмещение убытков (доходов в случае сохранения КТ) и пресечение действий, нарушающих права

12. Правовая защита от компьютерных преступлений.

КП включают:

1. Перехват информации.
2. НСД к информации.
3. Манипуляция данными и управляющими командами.
4. Вирусы.
5. Использование специальных программных средств.
6. Комплексные методы.

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

Составы КП даны в след статьях:

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

1. Неправомерный доступ к комп информации, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ – штраф до 200.000 р или в размере зарплаты до 18 месяцев, либо исправительные работы от 6 месяцев до 1 года, либо лишение свободы до 2 лет.

2. То же деяние, совершенное организованной группой либо с использованием служебного положения –штраф от 100 до 300.000 р или зарплата от 1 до 2 лет, либо исправительные работы от 1 до 2 лет, либо арест от 3 до 6 месяцев, либо лишение свободы до 5 лет.

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

1. Создание программ или изменение существующих, приводящих к НС уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, и распространение таких программ–лишение свободы до 3 лет со штрафом до 200.000 р или зарплата до 18 мес**.**

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, –лишение свободы от 3 до 7 лет.

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

1. Нарушение правил эксплуатации ЭВМ лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред, – запрет определённых должностей или деятельности до 5 лет, либо работы от 180 до 240 часов, либо ограничение свободы до 2 лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – лишение свободы до 4 лет.

13. Правовые основы деятельности службы безопасности.

Служба безопасности (СБ) фирмы – это структурное подразделение, которое обеспечивает защиту интересов фирмы в условиях коммерческого риска и конкурентной борьбы.

Законы РФ: «О частной детективной и охранной деятельности» от 11.03.1992 г.№ 2487-1, «О безопасности» от 28.12.2010 г. № 390-ФЗ, «Об оружии» от 13.12.1996 г. № 150-ФЗ, «Об информации, информационных технологиях и о защите информации» от 27.13.2006 г. № 149-ФЗ и Трудовой Кодекс.

Постановления Правительства РФ: «Вопросы частной детективной (сыскной) и частной охранной деятельности» от 14.08.1992 г. № 587, «Об организации ведомственной охраны» от 12.07.2000 г. № 514.

Устав фирмы, трудовые договоры, перечень сведений, составляющих КТ.

Согласно закону № 2487–1 частная детективная и охр деятельность требует лицензию (ст. 1) от органа внутренних дел.

В целях охраны разрешены услуги: защита жизни, охрана объектов и имущества в собственности и с осуществление работ по проектированию и обслуживанию тех. ср-в охраны, консультирование, обеспечение порядка, пропускного режима.

Частным детективам можно: устный опрос (с соглашения), внешний осмотр объектов, изучение предметов и док-в (с письменного согласия), наблюдение, съемка (фото, аудио, видео), соблюдать Зак-во РФ в части защиты информации, затрагивающей личную жизнь, применять СТС.

Частным детективам нельзя: скрывать факты преступлений от право-х орг-в, выдавать себя за их сотрудника, снимать в служебных помещениях, фальсифицировать материалы, собирать сведения о личной жизни, совершать действия, посягать на права людей, передавать лицензию, разглашать сведения о заказчике.

Частным детективам нужно: быть 21+, не стоять на учете по алк, нарк и псих, не иметь судимостей, не быть уволенным с гос. службы по компрометирующим их основаниям, не быть бывшим работником правоохранительных органов.

Лицензия частного охранника на 5 лет, для продления пройти профессиональное обучение по повышению квалификации частных охранников.

Частная охранная организация создается в форме ООО, осуществляет ТОЛЬКО охранную деятельность.

Руководитель ЧОО – имеет высшее образование, доп. проф. образование по повышению квалификации и иметь удостоверение частного охранника.

Частным охранникам можно: применять СТС и огнестрельное оружие: предупредить, стремиться к мин ущербу, оказать первую помощь пострадавшим, уведомить прокурора о смерти и причинении телесных повреждений.

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 охранником действий, повлекших нарушение прав граждан или интересов общества или государства, - штраф от 100 – 300.00 р или зарплата от 1 до 2 лет, либо ограничение свободы до 2 лет, либо принудительные работы до 2 лет с запретом определённых должностей или деятельности до 3 лет

2. То же, но с применением насилия или его угрозой или с оружием и повлекшее тяжкие последствия, - лишение свободы до 7 лет с запретом определённых должностей или деятельности до 3 лет.

14. Правовые основы использования технических средств сбора и защиты информации.

Специальные Технические Средства (СТС) – телефоны, принтеры, ТВ, сигнализации, кондиционер, радиомикрофон (жучок), стетоскоп (слух через стены, стекла, батареи), направленный микрофон (150м), микрокамеры.

УК РФ ст. 138. «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных сообщений граждан – штраф до 80.000 р или зарплата до 6 месяцев, либо работы до 360 ч, либо исправительные работы до 1 года.

2. То же деяние, совершенное с использованием служебного положения, –штраф от 100 до 300.000 р или зарплата от 1 до 2 лет, либо запрет определённых должностей или деятельности от 2 до 5 лет, либо обязательные работы до 480 ч, либо принудительные работы до 4 лет, либо арест до 4 месяцев, либо лишение свободы до 4 лет.

Указ Президента РФ №21 от 09.01 1996 г. «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в РФ и вывоза за ее пределы, а также использования СТС, предназначенных для негласного получения информации» возлагает на ФСБ:

– выдачу разрешений на деятельность и контроль в области СТС;

– лицензирование деятельности лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, продажей, ввозом в РФ и вывозом СТС, а также сертификацию, регистрацию и учет СТС;

– выявление случаев проведения неуполномоченными лицами оперативно - розыскных мероприятий и использования СТС.

Постановлением Правительства от 12.04.2012 г. № 287 введено "Положение о лицензировании деятельности по **разработке, производству, реализации и приобретению в целях продажи** (**РПРП**) СТС для негласного получения информации" Лицензируемая деятельность:

а) РПРП СТС для регистрации акустической информации;

б) для визуального наблюдения;

в) для прослушивания телефонных переговоров;

г) для перехвата информации с технических каналов связи;

д) для контроля почтовых отправлений;

е) для исследования предметов и документов;

ж) для обследования помещений, ТС и др;

з) для контроля за перемещением ТС и др;

и) для получения информации с технических средств ее хранения, обработки и передачи;

к) для идентификации личности.

Частным детективам нельзя использовать СТС.

15. Правовая основа системы лицензирования и сертификации в РФ.

Государственная система защиты информации (ГСЗИ) – органы, исполнители, техника защиты информации, объекты защиты. ГСЗИ функционирует по правилам, установленным нормативными документами в области ЗИ. **Является** составной частью системы обеспечения нац. безопасности РФ. **Призвана** защищать гос-во от внешних и внутренних угроз в информационной сфере. Организацию деятельности ГСЗИ осуществляет ФСТЭК.

ГСЗИ включает:

– органы (ФСБ, ФСТЭК, СБ), силы и средства, осуществление деятельность в области ЗИ;

– систему лицензирования деятельности в области ЗИ;

– систему сертификации средств ЗИ;

– систему (пере)подготовки специалистов в области ЗИ.

Лицензирование – это процесс передачи или получения физ/юр лицами прав на проведение работ. Получить право может только субъект, отвечающий критериям правил лицензирования.

Лицензия – документ, дающий право на осуществление указанного вида деятельности в течение определённого времени.

Виды деятельности в области ЗИ, на которые выдаются лицензии, определен **Постановлением Правительства РФ от 04.05.2011 № 99-ФЗ** "Об организации лицензирования отдельных видов деятельности:

1)разработка, распространение криптосредств, инф систем (ИС) и ТКС с криптозащитой, оказание услуг в области шифрования информации, ТО криптосредств, ИС и ТКС).

2) разработка и приобретение для продажи СТС для негласного получения информации;

3) деятельность по выявлению электронных устройств негласного получения информации;

4) разработка и производство средств защиты конфиденциальной информации;

5) деятельность по технической защите конфиденциальной информации.

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

Нормативная база лицензирования и сертификации

Законы РФ: - "О государственной тайне" от 21.07.1993 г. № 5485-1; - "О техническом регулировании" от 27.12.2002 г. № 184-ФЗ; - "О лицензировании отдельных видов деятельности" от 04.05.2011 г. № 99-ФЗ; - "О защите прав потребителей" от 07.02.1992 г. № 2300-1.

Постановления Правительства РФ: - "Об организации лицензирования отдельных видов деятельности" от 21.11.2011 г. № 957; - "О сертификации средств ЗИ" от 26.06.1995 г. № 608. - "О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации" от 03.03.2012 г. № 171. - "О лицензировании деятельности по технической защите конфиденциальной информации" от 03.02.2012 г. № 79.

16. Лицензирование деятельности по защите государственной тайны.

Общие нормы содержатся в ст. 27 "Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну" Закона "О государственной тайне"

Основные положений данной статьи:

– Для работы с ГТ нужна **лицензия**, она выдается только на основании результатов специальной экспертизы (проверки готовности организации к работе со сведениями, составляющими государственную тайну);

– в структуре организации должно быть подразделения по защите государственной тайны (ГТ) и специально подготовленные сотрудники;

– организация должна иметь сертифицированные средства защиты информации;

– необходима государственная аттестация руководителей организации, ответственных за защиту государственных секретов.

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 за границей;

– органами, уполномоченными на ведение лицензионной деятельности, являются: ФСБ, СВР (осуществлять допуск, оказание услуг), ФСТЭК, МО (осуществлять проведение работ по ср. защиты),

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

Продление срока действия лицензии производится в порядке, установленном для ее получения. На каждый вид деятельности выдается отдельная лицензия.

Специальные экспертизы предприятий выполняются по следующим направлениям:

– режим секретности;

– противодействие иностранной технической разведке;

– защита информации от утечки по техническим каналам.

Принципы лицензирования:

1) Лицензирование в области защиты ГТ является обязательным.

2) Деятельность в области ЗИ лиц, не прошедших лицензирование, запрещена

3) Лицензии на право деятельности в области ЗИ выдаются только юридическим лицам (физические лица не в состоянии удовлетворить указанным требованиям).

4) Лицензии выдаются только предприятиям, зарегистрированным на территории РФ на основании специальной экспертизы заявителя.

Для получения лицензии предприятие обязано предъявить следующий перечень документов.

– 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.

Основная **цель государственной аттестации** – повысить компетентность руководителей в части обеспечения сохранности сведений, составляющих государственную тайну.

17. Сертификация средств защиты информации.

Системы сертификации – это системы норм, правил, критериев качества продукции, методов их выявлений и оценки соответствия необходимым параметрам

Национальный орган по сертификации определяется Правительством РФ. В настоящее время эти функции выполняет Федеральное агентство по техническому регулированию и метрологии.

Сертификация средств защиты информации подразумевает проверку их качественных характеристик для реализации основной функции – защиты информации на основании государственных стандартов и требований по безопасности информации.

Самыми важными системами обязательной сертификации в России являются: ГОСТ Р, санитарно-эпидемиологическая, пожарная

Общие принципы сертификации средств защиты ГТ определены законом "О государственной тайне" и “ Положение о системе сертификации средств ЗИ (Приказ ФСТЭК)” – средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации СЗИ возлагается на ФСТЭК, ФСБ и МО в соответствии с функциями, возложенными на них законодательством Российской Федерации.

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.

Сертификации в системе сертификации ФСТЭК России подлежат средства противодействия иностранным разведкам, средства контроля разведке, средства технической ЗИ, средства обеспечения безопасности ИТ.

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.

Испытательные лаборатории проводят сертификационные испытания средств защиты информации и по их результатам оформляют технические заключения и протоколы. Испытательные лаборатории должны обеспечивать полноту

сертификационных испытаний средств защиты информации и достоверность их результатов

18. Аттестация объектов информатизации по требованиям безопасности информации.

Аттестация объектов информатизации по требованиям безопасности информации **осуществляется системой аттестации объектов информатизации по требованиям безопасности информации,** являющейся составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Возглавляет ФСТЭК России

Деятельность по аттестации объектов информатизации в названной системе осуществляется в соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации», утвержденным председателем Государственной технической комиссии при Президенте РФ 25.11.1994 г.

Аттестацией объектов информатизации – комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Обязательной аттестации подлежат объекты информатизации с ГТ, управления экологически опасными объектами, ведения секретных переговоров.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа (вирусов, ПЭМИН (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки по техническим каналам).

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации. Оплачивает заявитель.

Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, **выводом** о возможности

выдачи «Аттестата соответствия» и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя.

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод. Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания. Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

Если **объект информатизации соответствует** требованиям по безопасности информации, органом по аттестации выдается «Аттестат соответствия» на этот объект заявителю.

«Аттестат соответствия» выдается **не более чем на 3 года**. Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

В случае **изменения** условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

19. Лицензирование и сертификация в области защиты конфиденциальной информации.

Лицензирование деятельности в области защиты конфиденциальной информации основано на Законе РФ «О лицензировании отдельных видов деятельности» от 8 августа 2001 г. N 128-ФЗ (ред. от 11 марта 2003 г. N 32-ФЗ).

Лицензирование – деятельность лицензирующих органов по предоставлению лицензий, продлению срока, оценке, формированию и ведению реестра лицензий и тд.

Лицензия – специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности

Лицензирующие органы – уполномоченные федеральные органы исполнительной власти и (или) их территориальные органы, осуществляющие лицензирования в рамках полномочий субъектов РФ.

Лицензиат – юридическое лицо, владеющее лицензией.

В соответствии с настоящим Федеральным законом **лицензированию подлежат** следующие виды деятельности в области ЗИ

– разработка, производство, распространение, техническое обслуживание и предоставление услуг в области шифрования информации, специальных технических средств, предназначенных для негласного получения информации

– деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей и подтверждению подлинности электронных цифровых подписей;

– деятельность по выявлению электронных устройств, предназначенных для негласного получения информации.

– деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

– деятельность по технической защите конфиденциальной информации;

Проводятся **плановые проверки** лицензиата (по соблюдению лицензионных требований, по ФЗ «О государственном контроле (надзоре) и муниципальном контроле в РФ») после 1 и 3 лет выдачи лицензии, а также внеплановые.

Постановление Правительства РФ от 03.02.2012 г. № 79 утвердило «Положение о лицензировании деятельности по технической защите конфиденциальной информации», где определён порядок лицензирования. Его осущ ФСТЭК. Также есть Постановление «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации», где определено порядок лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации

Последовательность действий:

1) Прием лицензирующим органом заявления о предоставлении 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

Сертификация СЗИ – это процесс, направленный на подтверждение соответствия СЗИ нормам и требованиям, действующим на территории России

Сертификация СЗИ КИ проводится в соответствии с Положением "О сертификации средств защиты информации", утвержденным ПП РФ от 26.06.1995 г. № 608. Оно устанавливает порядок сертификации средств защиты информации в РФ.

Сертификации предусматривают комплекс мероприятий по проверке соответствия этих средств формальным базовым требованиям по обеспечению безопасности информации, изложенным в нормативных документах ФСТЭК.

20. Нормы ответственности за правонарушения в информационной сфере.

В законодательных актах установлены правовые нормы в отношении прав, обязанностей и ответственности субъектов, участвующих в информационном обмене.

Предметом правового регулирования в информационной сфере являются:

– создание и распространение информации;

– формирование и использование информационных ресурсов;

– реализация права на поиск, получение, передачу и потребление информации;

– создание и применение информационных систем и технологий;

– создание и применение средств информационной безопасности.

Ответственность формулируется в различных нормативных правовых актах. Конкретные нормы, устанавливающие ответственность за нарушения сосредоточены в УК, ГК, АК.

Уголовное право регулирует отношения в области наиболее опасных правонарушений – преступлений. Санкции за нарушение информационных правоотношений представлены в УК следующими статьями.

1) **Статья 138.** Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (штраф до 80к или зп за 6м, работы 360ч, при служебном полож до 300к или зп до 2х лет, лишение должности)

2) **Статья 140**. Отказ в предоставлении гражданину информации (до 200к или зп до 18м, лишение должности)

3) **Статья 183**. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну (обман до 500к или зп 12м, работы 12 м или 2 года, лишение свободы, без согласия до 1кк или зп 24м, лишение должности, работы 2г, 4г, лишение свободы)

4) **Статья 272**. Неправомерный доступ к компьютерной информации (если данные постарадли до 200к или зп 18м, работы 12м лишение 2 года, крупный ущерб до 300к или зп до 24м, работы 24м, лишение 4 г)

5) **Статья 273.** Создание, использование и распространение вредоносных программ для ЭВМ (лишение свободы 4г со штрафом до 200к, работы 4г)

6) **Статья 274.** Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (до 500к или зп 18м, работы до 12м, лишение св до 2г)

7) **Статья 275**. Государственная измена (лишение св 20л, 500к или зп до 3г, пожизенное)

8) **Статья 276**. Шпионаж (лишение св от 10 до 20л)

9) **Статья 283**. Разглашение государственной тайны (арест до 6м, лишение до 4г, лишие должности)

10) **Статья 284**. Утрата документов, содержащих государственную тайну (лишение до 3г, арест до 6м, лишение должнсти)

21. Защита информации от неправомерных действий органов, занимающихся оперативно- розыскной деятельностью.

Деятельность этих органов основывается на Законе РФ “Об оперативно-розыскной деятельности”, от 12.08.1995 г. № 144-ФЗ.

Оперативно-розыскная деятельность (ОРД) – вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим ФЗ, в пределах их полномочий посредством проведения оперативно розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств. **Задачи ОРД**:

1) выявление, предупреждение, пресечение и раскрытие преступлений;

2) осуществление розыска лиц скрывающихся

3) добывание информации о действиях, угрожающих государству;

4) установление имущества для взыскания и конфискации.

ОРД основывается на конституционных принципах законности, уважения и соблюдения прав и свобод человека и гражданина, а также на принципах конспирации, сочетания гласных и негласных методов и средств.

Оперативно-розыскными мероприятиями предусматривается:

Опрос, Наведение справок, Сбор образцов для сравнительного исследования, Проверочная закупка, Исследование предметов и документов. Наблюдение, Отождествление личности. Обследование помещений, зданий, сооружений, участков местности и транспортных средств, Контроль почтовых отправлений, телеграфных и иных сообщений, Прослушивание телефонных переговоров, Снятие информации с технических каналов связи, Оперативное внедрение, Контролируемая поставка, Оперативный эксперимент, Получение компьютерной информации.

В ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде.

Органам, осуществляющим ОРД, запрещается:

1) Проводить ОРМ в интересах партии и подобного;

2) принимать негласное участие в работе органов гос. власти и органов местного самоуправления;

3) разглашать сведения, затрагивающие неприкосновенность частной жизни, личную, семейную тайну и подобное;

4) подстрекать к совершению противоправных действий;

5) фальсифицировать результаты оперативно-разыскной деятельности.

Полученные в результате ОРД материалы в отношении лиц, виновность которых не доказана, **хранятся 1 год**, а затем уничтожаются. **Материалы, полученные в результате прослушки лиц**, в отношении которых не была возбуждена уголовка, уничтожаются в течение **шести месяцев** с прекращения прослушки.

Основания для проведения ОРМ:

1) Уголовное дело;

2) Сведения о подготавливаемом преступлении, событиях, создающих угрозу государству, лицах, скрывающихся от дознания или без вести пропавших, и об обнаруженных неопознанных трупов.

3) По запросу других органов;

4) Получения следователя, дознователя, органа дознания или определения суда по уголовным делам и материалам проверки сообщений о преступлении, находящимся в их производстве;

5) Постановлении о применении мер безопасности;

6) Запросы международных правоохранительных организаций**.**

Право осуществлять ОРД на территории РФ предоставляется оперативным подразделениям:

1. Органов внутренних дел РФ.

2. Органов ФСБ.

3. Федерального органа исполнительной власти в области государственной охраны.

4. Таможенных органов РФ.

5. Службы внешней разведки РФ.

6. Федеральной службы исполнения наказаний.

Контроль за ОРД осуществляют Президент, Федеральное Собрание РФ и Правительство РФ в пределах полномочий.

СОРМ – это комплекс технических средств и мер, предназначенных для проведения оперативно-разыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи. СОРМ обеспечивает два режима передачи информации: - передача статистической информации; - передача полной информации.

22. Защита коммерческой информации от неправомерных действий контролирующих и правоохранительных органов.

Законы, регламентирующие работу: 1. Закон РФ “О защите конкуренции” от 26.07.2006 г. № 135-ФЗ. 2. Закон РФ “О конкуренции и ограничении монополистической деятельности на товарных рынках”, от 22.03.1991 г. № 948-1. 3. Закон РФ “О полиции” от 07.02.2011 г. № 3-ФЗ. 4. Закона РФ “О санитарно-эпидемиологическом благополучии населения” от 30.03.1999 г. № 52-ФЗ. 5. Закон РФ

“О банках и банковской деятельности” от 01.12.1990 г. № 395-1 (в ред. ФЗ от 03.02.1996 г. № 17-ФЗ).

Одной из форм недобросовестной конкуренции, согласно закону “О защите конкуренции”, является недобросовестная конкуренция, связанная с **незаконным получением**, использованием или разглашением информации, составляющей коммерческую или иную охраняемую законом тайну.

К числу контролирующих органов относится федеральный антимонопольный орган, который имеет свои территориальные управления. **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.

Сотрудники полиции 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 полиции сведений, объясняющих необходимость вхождения на предприятие.

Государственный контроль за деятельностью полиции осуществляют Президент РФ, палаты Федерального Собрания РФ, Правительство РФ в пределах полномочий. **Прокурорский надзор за исполнением полицией** законов осуществляют Генеральный прокурор РФ и подчиненные ему прокуроры в соответствии с полномочиями.

Значительными полномочиями по проверке соблюдения на предприятиях санитарных правил, норм и гигиенических нормативов обладают должностные лица

и специалисты Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор).

Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

23. Сведения конфиденциального характера.

В действующем законодательстве РФ упоминается более 40 видов тайн (банковская, налоговая, коммерческая, профессиональная и т.д.),

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

«Перечень сведений конфиденциального характера» (по Указу пр РФ), где указаны: Коммерческая тайна, Служебная тайна, Профессиональная тайна, Персональные данные, Тайна следствия и судопроизводства, Сведения о защищаемых лицах и мерах государственной защиты, Сведения о сущности неопубликованных изобретений.

Однако, данный перечень может быть утвержден только законом в соответствии с нормами международного права и Конституции РФ. Отсутствие в законах четких определений видов информации с ограниченным доступом (за исключением государственной тайны) приводит к противоречиям между данным указом и существующими законодательными актами, что затрудняет их исполнение. **Например**, в действующих кодексах есть такие понятия как личная, семейная тайны и неприкосновенность частной жизни, а в других законах - **персональные данные**.

В действующих законах нет понятия «**тайна следствия и судопроизводства**», но есть понятия «данные предварительного расследования», «данные предварительного следствия», «тайна совещания судей», «тайна совещания присяжных заседателей».

В законах не дается понятия **служебной тайны** и в то же время применяется понятие «служебная информация». Соотношение между ними не установлено, а в указе вводится категория только служебной тайны. В действующем законодательстве наименее разработанными являются профессиональная тайна и служебная тайна.

Для обозначения грифа конфиденциальности используются международные и национальные нормативные документы. Причем требования российского законодательства отличаются от международных стандартов. **На основе российского законодательства** предпочтительнее применять следующее разграничение информации по грифу конфиденциальности:

1) открытая информация (ОИ);

2) для внутреннего использования (ДВИ);

3) конфиденциальная информация (КИ).

24. Нормативно-правовое регулирование профессиональной тайны.

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

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

В соответствии с определением профессиональной тайны выделяются следующие объекты профессиональной тайны:

1) **Врачебная тайна** – информация, содержащая: - результаты обследования лица, вступающего в брак; - сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья.

2) **Тайна связи** – тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

3) **Нотариальная тайна** – сведения, доверенные нотариусу в связи с совершением нотариальных действий.

4) **Адвокатская тайна** – сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи.

5) **Тайна усыновления** – сведения об усыновлении ребенка усыновителем.

6) **Тайна страхования** – сведения о страхователе, застрахованном лице и выгодоприобретателе.

7) **Тайна исповеди** – сведения, доверенные священнослужителю гражданином на исповеди.

8) **Журналистская тайна** – сведения, сообщенные журналисту.

Например профессиональную тайну можно найти в ГК РФ (Охрана частной жизни гражданина); УК РФ (Разглашение тайны усыновления (удочерения)); ГПК РФ (Гласность судебного разбирательства); УПК РФ (Полномочия защитника);

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).

25. Нормативно-правовое регулирование служебной тайны.

Должностная служебная тайна связана с интересами государственной службы и службы в органах местного самоуправления. Доступ к служебным сведениям закрытого характера связан с должностным статусом лиц, которым эти сведения стали известны по службе. Поэтому при утечке этой информации страдают интересы службы (а не клиентов, как в случае профессиональной тайны).

Служебная тайна – это защищаемая конфиденциальная информация, доступ к которой ограничен законом (Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера»), ставшая известной сотрудникам организаций при исполнении ими служебных обязанностей.

Примерами противоправных действий являются: разглашение судьями тайны совещания при вынесении приговора, должностными лицами Банка России банковской тайны, работниками налоговой инспекции налоговой тайны (сведения о налогоплательщике).

Служебная тайна не относится к коммерческой тайне. **Обязанность работника не разглашать коммерческую или служебную тайну** может быть установлена в трудовом договоре, должностной инструкции или в отдельном положении о служебной тайне.

Служебная тайна регулируется актами специального назначения, которые направлены на деятельность работников государственного аппарата, *а* профессиональная тайна, в свою очередь, направлена на широкий круг специалистов и регулируется отдельным профильными законами.

Служебная тайна относится к конфиденциальной информации. **Поэтому закон предъявляет к ней особые меры защиты**. Так, в целях защиты служебной информации необходимо принять меры, которые должны обеспечить: 1) защиту от несанкционированного доступа, копирования, уничтожения, внесения изменений, блокирования и тиражирования сведений, составляющих служебную тайну; 2) сохранение конфиденциальности; 3) реализацию права на доступ только ограниченному кругу лиц, имеющих официальное разрешение.

Условия отнесения информации к служебной тайне определяет закон. Можно выделить три критерия, по которым информация может быть отнесена к служебной тайне: 1) она не составляет государственную тайну; 2) она не является общедоступной; 3) обеспечить ее сохранность и ограничить несанкционированный доступ можно в режиме профессиональной или служебной тайны.

Доступ к документам, которые содержат служебную тайну, работникам учреждения производится только под расписку. **Все документы, которые содержат конфиденциальные сведения,** должны иметь соответствующую пометку: «для служебного пользования».

За разглашение служебной тайны для должностных лиц предусмотрена различная ответственность. В первую очередь, **Трудовым кодексом** установлено право работодателя применить в случае разглашения работником охраняемой тайны дисциплинарное взыскание вплоть до увольнения (п. 6 ст. 81 ТК РФ). В этом случае в трудовой книжке указывается причина увольнения со ссылкой на статью ТК РФ.

В ст. 13.14 **КоАП также предусмотрено наказание за разглашение информации с ограниченным доступом**: - для граждан штраф составляет от 500 руб. до 1000 руб.; - для должностных лиц — от 4000 руб. до 5000 руб.

26. Правовое обеспечение защиты персональных данных.

Персональные данные – информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу

Правовой защите подлежит лишь та информация о человеке, которая позволяет его персонифицировать. И ФЗ «О персональных данных» и европейский Регламент определяют персональные данные достаточно широко, поэтому какого-либо перечня сведений, относящихся к персональным данным субъекта, не существует.

Меры по защите ПД были вызваны высоким уровнем хищения информации инсайдерами и несоответствие правовых норм защиты ПД в России и Евросоюзе, мешающее развитию торговли севропейскими странами.

Утечки данных определяются **внутренними** угрозами информационной безопасности из-за сотрудников (инсайдеров), работающих на конкурентов, связанных с криминалом, недобросовестных, обиженных на начальство и халатных)

Самыми «популярными» персональными данными среди инсайдеров являются детали конкретных сделок, финансовые отчеты, интеллектуальная собственность компании, бизнес-планы

Каналы утечки данных: Мобильные накопители, Электронная почта, Интернет-мессенджеры, Интернет (web-почта, форумы, блоги), Принтеры, Фото-видеоустройства.

Конвенция и последовавшие за ней Директивы Евросоюза сформулировали **задачи**, которые должно регулировать национальное законодательство в отношении ПД:

– защита ПД от НСД к ним со стороны других лиц, в том числе представителей государственных органов и служб, не имеющих на то необходимых полномочий;

– обеспечение сохранности, целостности и достоверности данных в процессе работы с ними

– обеспечение надлежащего правового режима этих данных при работе с ними для различных категорий ПД;

– обеспечение контроля над использованием ПД со стороны самого гражданина

Принципы обработки персональных данных (ст. 5 ФЗ о ПД):

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

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

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

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

Условия обработки персональных данных (ст. 6 ФЗ о ПД):

1) Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим ФЗ (с согласия субъекта, необходима для целей по законам РФ, осущ в связи с участием субъекта в судопроизводтсве, для исполнения полномочий федеральных органов исполнительной власти, для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, для защиты жизни, здоровья или иных жизненно важных интересов, в статистических или иных исследовательских целях)

2) Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего ФЗ

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

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

Оператор ПД волен производить с ПД сбор, запись, систематизацию, хранение, уточнение, использование, передача (только по соглашению с субъектом), удаление

ПД бывают обычные, разрешённые для распространения, специальные (раса, нация, полит взгляды), биометрические.

Безопасность ПД достигается путем исключения несанкционированного, в том числе случайного, доступа к ним. **Обмен ПД** при их обработке в информационных системах осуществляется по защищенным каналам связи.

27. Международные стандарты и соглашения в области безопасности информационных технологий.

Важным элементом решения проблемы безопасности ИТ является выработка системы требований, критериев и показателей для оценки уровня безопасности ИТ в виде **международного стандарта**

В 1990 г. Международная организация по стандартизации (ISO) начала разработку **международного стандарта критериев оценки для общего использования** – Международный стандарт ISO/IEC 15408-99 "**Критерии оценки безопасности информационных технологий**". Был создан на основе предыдущих документов («Оранжевая книга» США (1985), канадские (1993) и европейские (1991), критерии на базе американских «Критериев оценки доверенных компьютерных систем (1991))

Действующим национальным стандартом является ГОСТ Р ИСО/МЭК 15408-1-2012 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 814-ст). **Содержит** общие критерии (ОК) оценки безопасности информационных технологий. Предназначен в качестве руководства при разработке и при приобретении коммерческих продуктов или систем с функциями безопасности ИТ.

ОК применимы к мерам безопасности ИТ, реализуемым аппаратными, программно-аппаратными и программными средствами. **Критерии для оценки специфических качеств криптографических алгоритмов не входят в ОК.** Предназначены в основном для потребителей, разработчиков и оценщиков

В настоящее время действуют также и другие международные и российские стандарты

ISO/IEC 17799 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры обеспечения информационной безопасности»

ГОСТ Р ИСО/МЭК 13335-1-2006 "Информационная технология. Методы и средства обеспечения безопасности. Часть 1. И Часть 2»

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»

ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»

В Будапеште 23 ноября 2001 г. подписана **Конвенция** по борьбе с киберпреступностью. (26 европейских стран, а также Канады, США, ЮАР и Японии)

Конвенция разрабатывалась специальным комитетом Совета Европы при участии юристов США и других стран в течение четырех лет

Россия не подписала Конвенцию Совета Европы из-за пункта "b" статьи 32:

28. Особенности и классификация компьютерных преступлений.

Проблема: при расследовании многих преступлений в компьютерных системах **заключается** в установлении самого факта совершения преступления.

Особенность: чтобы утверждать, что было совершено преступление с использованием компьютера, необходимо доказать следующие факты:

– компьютерная информация, к которой произведен **несанкционированный доступ**, охраняется законами РФ;

– злоумышленником были осуществлены определенные **неправомерные действия**;

– этими несанкционированными действиями **нарушены права собственника** информации;

– несанкционированный **доступ к средствам компьютерной техники** либо попытка доступа;

– использование информации в **преступных целях**. Например, с целью совершения преступления. Тогда **доказыванию подлежит**

– совершение несанкционированных манипуляций с программным обеспечением (ПО), **что лицо совершало их с преступной целью**.

Комплекс следственных действий включает:

1. **Проведение обыска** в служебном помещении, на рабочем месте подозреваемого и изъятие физических носителей информации и других документов.

2. **Исследование** журнала рабочего времени ЭВМ, средств защиты и контроля регистрирующих систем пользователей, всего ПО ЭВМ, "прошитых" микросхем ПЗУ, микропроцессоров и т. п.

3. **Анализ указаний** по обработке ежедневной бухгалтерской информации.

4. **Допрос** инженеров, программистов и специалистов электронщиков, занимающихся эксплуатацией и ремонтов вычислительной техники.

5. Проведение комплексной **судебно-бухгалтерской и программно-технической экспертизы** с привлечением соответствующих специалистов правоохранительных органов.

Судебно-бухгалтерская экспертиза устанавливает **нарушения** в документообороте, **их причины** и **ответственные лица** за эти нарушения.

С помощью таких экспертиз решаются задачи: **Воспроизведение информации**, **Восстановление информации**, **Установление времени** действий с информацией, **Расшифровка закодированной информации**, **Установление авторства**, **Выяснения возможных каналов утечки** информации, **Выяснение технического состояния** носителей информации, **Установления уровня профессиональной подготовки** отдельных лиц, проходящих по делу в области программирования и в качестве пользователя.

Классификация способов совершения КП

По кодификатору **Интерпола** с 1991 г. все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы **Q**.

QA - Несанкционированный доступ и перехват

QD - Изменение компьютерных данных

QF - Компьютерное мошенничество

QR - Незаконное копирование

QS - Компьютерный саботаж

QZ - Прочие компьютерные преступления

Для характеристики преступления могут использоваться до пяти кодов. Например, несанкционированный доступ и перехват информации (QA) включает в себя следующие виды КП:

QAH – "Компьютерный абордаж" (неправомерный доступ в компьютер или сеть).

QAI – перехват: перехват при помощи технических средств.

QAT – кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.

29. Требования к безопасности компьютерных сетей в РФ.

Эти требования были разработаны бывшей ГТК РФ (Гостехкомиссия при Президенте Российской Федерации) и **обязательны** для государственных предприятий или для коммерческих предприятий допущенных к сведениям составляющих ГТ. В остальных случаях они носят рекомендательный характер.

Требования к безопасности АС устанавливаются в соответствии с классом защищенности. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. Т.е. установлено **9 классов защищенности** в трех группах:

3-я группа - в АС работает 1 пользователь, допущенный к информации одного уровня конфиденциальности; А – ГТ, Б – служебная тайна или ПД;

2-я группа – в АС пользователи имеют одинаковые права к информации различного уровня конфиденциальности; А – ГТ, Б – служебная тайна или ПД;

1-я группа – многопользовательские системы с доступом к информации разного уровня. А – гриф «Особая важность», Б – гриф «Совершенно секретно», В – гриф «секретно», Г – АС со служебной тайной, Д – АС с ПД;

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, **комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД** реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

– управления доступом;

– регистрации и учета;

– криптографической;

– обеспечения целостности

Показатели защищенности средств вычислительной техники от НСД даны в РД ГТК (Руководящие документы Гостехкомиссии при Президенте Российской Федерации) «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением председателя Государственной технической комиссии при Президенте РФ от 30.03.1992 г.)

РД устанавливает классификацию средств вычислительной техники (СВТ) по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

В данном РД определяется 7 классов защищенности средств вычислительной техники (СВТ) от НСД к информации.

Самый высокий – 1, самый низкий – 7 класс.

Классы подразделяются на 4 группы:

1 гр. включает – 7 кл., **2гр.** включает – 6 и 5 кл., **3 гр.** включает – 4, 3 и 2 кл., **4 гр.** включает – 1 кл.

Для присвоения класса защищенности АС должна иметь:

– руководство администратора по системе;

– руководство пользователя;

– тестовую и конструкторскую документацию.

Для корпоративных сетей с большим количеством пользователей составляется документ, регламентирующий работу в сети – «Политика безопасности». Это совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. **Обеспечивает выполнение** идентификации, разделения полномочий, регистрации и учета работы, шифрования, применения цифровой подписи, обеспечения антивирусной защитой, контроль целостности информации.

30. Объекты интеллектуальной собственности.

Интеллектуальная собственность – закрепленное законом временное исключительное право, а также личные неимущественные права авторов на результат интеллектуальной деятельности или средства индивидуализации.

Законодательство, определяющее права на интеллектуальную собственность, устанавливает монополию авторов на определенные формы использования результатов своей интеллектуальной, творческой деятельности, которые, таким образом, могут использоваться другими лицами лишь с разрешения первых.

В ст. 1225 ГК РФ «Охраняемые результаты интеллектуальной деятельности и средства индивидуализации» дается определение результатов интеллектуальной деятельности.

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

Произведения науки, литературы и искусства, программы, базы данных, фонограммы, изобретения, полезные модели, промышленные образцы, селекционные достижения, секреты производства, наименования, товарные знаки.

2. Интеллектуальная собственность охраняется законом.

Ст. 1226 ГК РФ Интеллектуальные права

На результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации признаются интеллектуальные права, которые включают **исключительное право**, являющееся имущественным правом, а в случаях, предусмотренных настоящим Кодексом, также личные неимущественные права и иные права (право следования, право доступа и другие).

Существует **три** общепризнанные в мире правовые **формы** защиты объектов интеллектуальной собственности (ОИС):

– 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 (форма правовой защиты любых полезных сведений (производственных, технических, экономических, организационных и других)).

Были созданы организации и союзы по охране ИС:

1) Объединенные международные бюро по охране интеллектуальной собственности (БИРПИ)–международная организация образована в конце 1892 г., предшественница Всемирной организации интеллектуальной собственности (ВОИС);

2) Всемирная Организация Интеллектуальной Собственности(ВОИС), основана 14.07.1967 г.;

3) **Международный союз по охране промышленной собственности (Парижский союз)**, образованный Парижской конвенцией по охране промышленной собственности от 20.03.1883 г.;

4) **Союз по охране прав авторов на их литературные и художественные произведения (Бернский Союз)**, образованный Бернской конвенцией по охране литературных и художественных произведений от 04.12.1887 г.

Автором результата интеллектуальной деятельности признается **гражданин**, творческим трудом которого создан такой результат. Ему же принадлежит право авторства, право на имя и иные личные неимущественные права.

Авторство и имя автора охраняются бессрочно.

Исключительное право на результат интеллектуальной деятельности, созданный творческим трудом, первоначально возникает у его автора.

Это право может быть передано автором другому лицу по договору, а также может **перейти к другим лицам** по иным основаниям, установленным законом.

Права на результат интеллектуальной деятельности, созданный совместным творческим трудом двух и более граждан, принадлежат соавторам совместно.

31. Правовая охрана авторских и смежных прав.

Авторские права регулируются Главой 70. Авторское право Части 4 ГК РФ.

Статья 1255 ГК РФ. Авторские права

1. Интеллектуальные права на произведения науки, литературы и искусства являются авторскими правами.

2. Автору произведения принадлежат следующие права:

а) исключительное право на произведение;

б) право авторства;

в) право автора на имя;

г) право на неприкосновенность произведения;

д) право на обнародование произведения.

Авторское право распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой-либо объективной форме:

- письменной;
- устной (выступление, исполнение и т. д.);
- звуко- или видеозаписи;
- изображения (рисунок, чертеж, теле-, фотокадр и т. д.);
- объемно-пространственной (скульптура, макет и т. д.);
- в других формах.

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

Автор – физическое лицо, творческим трудом которого создано произведение. Авторское право НЕ распространяется на идеи, методы, процессы, системы, концепции, принципы, открытия, факты.

Авторское право на произведение возникает в силу факта его создания. Для возникновения и осуществления авторского права не требуется регистрации произведения или соблюдения каких-либо формальностей. В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя (в соответствии с правилами ст. 1262 Гражданского Кодекса).

Обладатель исключительных *авторских прав* для оповещения о своих правах вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состоит из трех элементов: латинской буквы “С” в окружности ©; имени (наименования) обладателя исключительных прав; года первого опубликования произведения.

При соавторстве (произведение создано двумя и более лицами) авторское право принадлежит соавторам совместно, независимо от характера и структуры произведения (неразрывное целое или имеет отдельные самостоятельные части).

Авторское право действует в течение всей жизни автора и 70 лет после его смерти (п. 1 ст. 1281 ГК РФ).

Истечение срока действия авторского права на произведения означает их переход в общественное достояние (ст. 1282 ГК РФ). Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно.

Смежные права регулируются Главой 71. Права, смежные с авторскими Части 4 ГК РФ.

Статья 1304 ГК РФ. Объекты смежных прав

1. Объектами смежных прав являются:

а) результаты исполнительской деятельности (исполнения), к которым относятся исполнения артистов-исполнителей и дирижеров, если эти исполнения можно повторно публично исполнить при сохранении узнаваемости конкретной постановки зрителями, а также в форме, допускающей воспроизведение и распространение с помощью технических средств;

б) фонограммы;

в) сообщения передач организаций эфирного или кабельного вещания;

г) базы данных в части их охраны от несанкционированного извлечения и повторного использования составляющих их содержание материалов;

д) произведения науки, литературы и искусства, обнародованные после их перехода в общественное достояние.

2. Для возникновения, осуществления и защиты смежных прав не требуется регистрация их объекта или соблюдение каких-либо иных формальностей.

3. Предоставление на территории РФ охраны объектам смежных прав в соответствии с международными договорами РФ осуществляется: в отношении исполнений, фонограмм, сообщений передач организаций эфирного или кабельного вещания, не перешедших в общественное достояние в стране их происхождения вследствие истечения установленного в такой стране срока действия исключительного права на эти объекты и не перешедших в общественное достояние в РФ вследствие истечения предусмотренного настоящим Кодексом срока действия исключительного права.

Для включения механизма защиты смежных прав необходимо заявление обладателя прав о нарушении его прав (т. к. многие фирмы этого не делали, то до недавнего времени около 90% пиратской продукции на рынке считалось законной).

Обладатели исключительных или смежных прав вправе требовать от нарушителя: признания своих прав; возмещения убытков; взыскание полученного дохода; выплаты

компенсации в размере от 10 000 рублей до 5 млн рублей, определяемом по усмотрению суда.

Знак охраны *смежных прав* – латинская буква “Р” в окружности, имя обладателя прав и год первого опубликования фонограммы.

Исключительное право на исполнение действует в течение всей жизни исполнителя, но не менее 50 лет, считая с 1 января года, следующего за годом, в котором осуществлены исполнение, либо запись исполнения, либо сообщение исполнения в эфир или по кабелю.

По истечении срока действия исключительного права на исполнение это право переходит в общественное достояние. Исключительное право на фонограмму действует в течение 50 лет, считая с 1 января года, следующего за годом, в котором была осуществлена запись.

Статья 146 УК РФ. Нарушение авторских и смежных прав

1. Присвоение авторства (плагиат), если это деяние причинило крупный ущерб автору или иному правообладателю, - наказывается штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок от 180 до 240 часов, либо арестом на срок от 3 до 6 месяцев.

2. Незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере, - наказывается штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок до 480 часов, либо исправительными работами на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частью второй настоящей статьи, если они совершены:

а) группой лиц по предварительному сговору или организованной группой;

б) в особо крупном размере;

в) лицом с использованием своего служебного положения, - наказывается принудительными работами на срок до 5 лет либо лишением свободы на срок до 6 лет

со штрафом в размере до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до 3 лет или без такового.

32. Правовая охрана программ для ЭВМ и баз данных.

Статья 1261 ГК РФ. Программы для ЭВМ

Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы. Личные права автора на программу или базу данных охраняются бессрочно.

Программой для ЭВМ – является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Правообладатель для оповещения о своих правах может использовать знак охраны авторского права: буквы С в окружности или в круглых скобках ©; наименования (имени) правообладателя; года первого выпуска программы в свет.

Статья 1335 ГК РФ. Срок действия исключительного права изготовителя базы данных

1. Исключительное право изготовителя базы данных возникает в момент завершения ее создания и действует в течение 15 лет, считая с 1 января года, следующего за годом ее создания.

Исключительное право изготовителя базы данных, обнародованной в указанный период, действует в течение 15 лет, считая с 1 января года, следующего за годом ее обнародования.

2. Сроки, предусмотренные пунктом 1 настоящей статьи, возобновляются при каждом обновлении базы данных.

33. Технические средства защиты авторских прав.

Статья 1299 ГК РФ. Технические средства защиты авторских прав

1. Техническими средствами защиты авторских прав признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к

произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения.

2. В отношении произведений НЕ допускается:

а) осуществление без разрешения автора или иного правообладателя действий, направленных на то, чтобы устранить ограничения использования произведения, установленные путем применения технических средств защиты авторских прав;

б) изготовление, распространение, сдача в прокат, предоставление во временное безвозмездное пользование, импорт, реклама любой технологии, любого технического устройства или их компонентов в целях получения прибыли либо оказание соответствующих услуг

3. В случае нарушения положений, предусмотренных пунктом 2 настоящей статьи, автор или иной правообладатель вправе требовать по своему выбору от нарушителя возмещения убытков или выплаты компенсации в соответствии со статьей 1301 настоящего Кодекса.

4. В случае, если пунктами 1-3 статьи 1274 и статьей 1278 настоящего Кодекса разрешено использование произведения без согласия автора или иного правообладателя и такое использование невозможно осуществить в силу наличия технических средств защиты авторских прав, лицо, правомерно претендующее на осуществление такого использования, может требовать от автора или иного правообладателя снять ограничения использования произведения, установленные путем применения технических средств защиты авторских прав, либо предоставить возможность такого использования по выбору правообладателя при условии, что это технически возможно и не требует существенных затрат.

34. Охрана топологии интегральных микросхем.

Статья 1448 ГК РФ. Топология интегральной микросхемы

1. *Топологией интегральной микросхемы* - является зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов *интегральной микросхемы (ИМС)* и связей между ними. При этом *интегральной микросхемой* - является микроэлектронное изделие окончательной или промежуточной формы, которое предназначено для выполнения функций электронной

схемы, элементы и связи которого нераздельно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено такое изделие.

2. Правовая охрана распространяется только на оригинальную топологию интегральной микросхемы, созданную в результате творческой деятельности автора и неизвестную автору и (или) специалистам в области разработки топологий интегральных микросхем на дату ее создания. Топология интегральной микросхемы признается оригинальной, пока не доказано обратное.

3. Правовая охрана, предоставляемая настоящим Кодексом, не распространяется на идеи, способы, системы, технологию или закодированную информацию, которые могут быть воплощены в топологии интегральной микросхемы.

Статья 1449 ГК РФ. Права на топологию интегральной микросхемы

1. Автору топологии интегральной микросхемы принадлежат следующие интеллектуальные права:

а) исключительное право;

б) право авторства.

2. В случаях, предусмотренных настоящим Кодексом, автору топологии интегральной микросхемы принадлежат также другие права, в том числе право на вознаграждение за служебную топологию.

Статья 1450 ГК РФ. Автор топологии интегральной микросхемы

Автором топологии интегральной микросхемы признается гражданин, творческим трудом которого создана такая топология. Лицо, указанное в качестве автора в заявке на выдачу свидетельства о государственной регистрации топологии интегральной микросхемы, считается автором этой топологии, если не доказано иное.

Статья 1451 ГК РФ. Соавторы топологии интегральной микросхемы

1. Граждане, создавшие топологию интегральной микросхемы совместным творческим трудом, признаются соавторами.

2. Каждый из соавторов вправе использовать топологию по своему усмотрению, если между ними не предусмотрено иное соглашением.

3. К отношениям соавторов, связанным с распределением доходов от использования топологии и с распоряжением исключительным правом на топологию, соответственно применяются правила пункта 3 статьи 1229 настоящего Кодекса.

Распоряжение правом на получение свидетельства о государственной регистрации топологии интегральной микросхемы осуществляется соавторами совместно.

Статья 1455 ГК РФ. Знак охраны топологии интегральной микросхемы

Правообладатель для оповещения о своем исключительном праве на топологию вправе использовать знак охраны, который помещается на топологии, а также на изделиях, содержащих такую топологию, и состоит из: выделенной прописной буквы "Т" ("Т", [Т], Т*, буквы "Т" в окружности, или буквы "Т" в квадрате), даты начала срока действия исключительного права на топологию, информации, позволяющей идентифицировать правообладателя.

Право автора на топологию является неотъемлемым личным правом и охраняется законом бессрочно.

Исключительное право на использование топологии действует в течение 10 лет.

Автор топологии и иной правообладатель вправе требовать:

- признания прав;
- возмещения причиненных убытков.

За защитой своего права автор может обратиться в суд (арбитражный или третейский)

35. Охрана патентных прав.

Изобретение – техническое решение в любой области, относящееся к продукту (в частности, устройству, веществу и т. п.

Полезная модель – техническое решение, относящееся к устройству.

Промышленный образец – решение внешнего вида изделия промышленного или кустарно-ремесленного производства

Патентные права регулируются Главой 72. Патентное право Части 4 ГК РФ.

Статья 1345 ГК РФ. Патентные права

1. Интеллектуальные права на изобретения, полезные модели и промышленные образцы являются патентными правами.

2. Автору изобретения, полезной модели или промышленного образца принадлежат следующие права:

а) исключительное право;

б) право авторства.

3. В случаях, предусмотренных настоящим Кодексом, автору изобретения, полезной модели или промышленного образца принадлежат также другие права, в том числе право на получение патента, право на вознаграждение за служебное изобретение, полезную модель или промышленный образец.

Статья 1347 ГК РФ. Автор изобретения, полезной модели или промышленного образца

Автором изобретения, полезной модели или промышленного образца признается гражданин, творческим трудом которого создан соответствующий результат интеллектуальной деятельности. Лицо, указанное в качестве автора в заявке на выдачу патента на изобретение, полезную модель или промышленный образец, считается автором изобретения, полезной модели или промышленного образца, если не доказано иное.

Статья 1349 УК РФ. Объекты патентных прав

1. Объектами патентных прав являются результаты интеллектуальной деятельности в научно-технической сфере, отвечающие установленным настоящим Кодексом требованиям к изобретениям и полезным моделям, и результаты интеллектуальной деятельности в сфере дизайна, отвечающие установленным настоящим Кодексом требованиям к промышленным образцам.

2. На изобретения, содержащие сведения, составляющие государственную тайну (секретные изобретения), положения настоящего Кодекса распространяются, если иное не предусмотрено специальными правилами статей 1401-1405 настоящего Кодекса и изданными в соответствии с ними иными правовыми актами.

3. Полезным моделям и промышленным образцам, содержащим сведения, составляющие государственную тайну, правовая охрана в соответствии с настоящим Кодексом НЕ предоставляется.

4. НЕ могут быть объектами патентных прав:

а) способы клонирования человека и его клон;

б) способы модификации генетической целостности клеток зародышевой линии человека;

в) использование человеческих эмбрионов в промышленных и коммерческих целях;

г) результаты интеллектуальной деятельности, указанные в пункте 1 настоящей статьи, если они противоречат общественным интересам, принципам гуманности и морали.

Статья 134 ГК РФ. Патент на изобретение, полезную модель или промышленный образец

1. Патент на изобретение, полезную модель или промышленный образец удостоверяет приоритет изобретения, полезной модели или промышленного образца, авторство и исключительное право на изобретение, полезную модель или промышленный образец.

2. Охрана интеллектуальных прав на изобретение или полезную модель предоставляется на основании патента в объеме, определяемом содержащейся в патенте формулой изобретения или соответственно полезной модели. Для толкования формулы изобретения и формулы полезной модели могут использоваться описание и чертежи, а также трехмерные модели изобретения и полезной модели в электронной форме (пункт 2 статьи 1375 и пункт 2 статьи 1376).

3. Охрана интеллектуальных прав на промышленный образец предоставляется на основании патента в объеме, определяемом совокупностью существенных признаков промышленного образца, нашедших отражение на изображениях внешнего вида изделия, содержащихся в патенте на промышленный образец.

Присвоение авторства, принуждение к соавторству, незаконное разглашение сведений об объекте промышленной собственности влекут за собой уголовную ответственность в соответствии с законодательством РФ.

Публикация сведений о выдаче патента

Федеральный орган исполнительной власти по интеллектуальной собственности публикует в официальном бюллетене сведения о выдаче патента на изобретение, полезную модель или промышленный образец, включающие:

- имя автора (если автор не отказался быть упомянутым в качестве такового),

- имя или наименование патентообладателя,

- название и формулу изобретения или полезной модели либо перечень существенных признаков промышленного образца и его изображение.

Статья 147 УК РФ. Нарушение изобретательских и патентных прав

1. Незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб, - наказываются штрафом (в размере от 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок от 180 до 240 часов, либо лишением свободы на срок до 2 лет.)

2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, - наказываются штрафом (в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет, либо арестом на срок от 4 до 6 месяцев, либо лишением свободы на срок до 5 лет.)

ЧАСТЬ 2. КНЯЗЕВА

1. Управление рисками информационной безопасности. Идентификация и оценка технических уязвимостей. Расчет рисков по методике CVSS 3.0 Common Vulnerability Score System. Общая система оценки уязвимостей. Метрики CVSS 3.0. Основные пользователи системы. Описание базовых, временных и контекстных метрик. Как формируется вектор, описывающий уязвимость?

Ошибки в программном обеспечении, которые могут быть непосредственно использованы злоумышленником для реализации угроз безопасности, называют ***уязвимостями****.*

Ошибки, которые могут привести к возникновению уязвимостей – ***недостатками (слабостями) безопасности.***

CVE – база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер.

Управление рисками информационной безопасности по своей сути является ядром системы менеджмента информационной безопасности (СМИБ).

Составляющими процесса управления рисками являются процедуры своевременного **выявления рисков**, их **оценка** и последующая **обработка**.

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.

Для оценки рисков уязвимостей технических информационных систем применяются различные **подходы**:

– системы оценки угроз;

– базы данных уязвимостей (NVD, OSVDB);

– системы идентификации уязвимостей (CVE, CWE).

Системы оценки уязвимостей:

1. **DREAD:** D – damage potential; R – reproducibility; E – exploitability; A – affected users; D – discoverability.

2. **CVSS 3.0** (уже есть 4.0).

Пользователи CVSS:

– Поставщики бюллетеней с описанием уязвимости;

– Разработчики программных приложений;

– Организации-пользователи;

– Сканирование уязвимостей и управление уязвимостями;

– Управление (рисками) безопасности;

– Исследователи.

Общая система оценки уязвимостей (вообще то «Система оценки общих уязвимостей») [Common Vulnerability Scoring System, CVSS], текущая версия 3.1 – **открытая схема для обмена и оценки уязвимостей ИТ.** В этой системе используются группы метрик, а также дается описание базовых метрик, вектора уязвимости и оценок уязвимости.

Группы метрик CVSS 3.0:

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

Временные метрики [temporal]: при оценке метрики учитывается время, например опасность уязвимости снижается с выходом официального обновления безопасности.

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

БАЗОВЫЕ подразделяются на метрики **эксплуатации [exploitability]** и **воздействия [impact]**:

ЭКСПЛУАТАЦИИ:

1. Вектор атаки [Attack Vector, AV]:

– **Сетевой [Network]** –удалённо через сеть (путь через 3-й уровень OSI);

– **Соседский [Adjacent]** – из соседней локальной сети (без 3-го уровня OSI, без прохождения через маршрутизатор);

– **Локальный [Local]** – из локальной сети;

– **Физический [Physical]** – непосредственный доступ к устройству/системе.

2. Сложность доступа [Access Complexity, AC]:

– **Low** – нет спец. условий и особых обстоятельств.

– **High** – успех зависит от условий, на которые злоумышленник не может повлиять.

3. Требуемые привилегии [Privileges Required, PR]:

– **None** – нет необходимости в авторизации.

– **Low** – любые базовые привилегии.

– **High** – требуются права администратора.

4. Взаимодействие с пользователем [User Interaction, UI]:

– **None** – не требуется взаимодействие злоумышленника с другим авторизованным пользователем или запущенным процессом.

– **Required** – для эксплуатации требуются действия со стороны другого пользователя.

5. Область действия [Scope]:

– **Unchanged** – воздействие уязвимости в пределах ресурсов компонента.

– **Changed** – воздействие уязвимости в компоненте на ресурсы за рамками привилегий, которыми наделен этот компонент.

ВОЗДЕЙСТВИЯ:

1. Воздействие на конфиденциальность [Confidentiality Impact, C]:

– **High** – полная потеря конфиденциальности.

– **Low** – частичная.

– **None** – нет потерь.

2. Воздействие на целостность [Integrity Impact, I]:

– Как и в конфиденциальности.

3. Воздействие на доступность [Availability Impact, A]:

– Как и в конфиденциальности.

ВРЕМЕННЫЕ метрики:

4. Зрелость кода эксплойта [Exploit Code Maturity, E]:

– **Not Defined** – не влияет на оценку.

– **High** – существует функциональный автономный код (не нужен эксплоит, уязвимость и так доступна)

– **Functional** – существует рабочий эксплойт.

– **Proof-of-Concept** – концепция эксплойта верна, но не всегда применима, нужна модификация.

– **Unproven** – кода эксплойта нет или эксплуатация возможна только в теории.

5. Уровень устранения [Remediation Level, RL]:

– **Not Defined** – не влияет на оценку.

– **Unavailable** – нет решения для уязвимости.

– **Workaround** – неофициальный патч от третьей стороны.

– **Temporary Fix** – официальный временный патч.

– **Official Fix** – полное официальное исправление.

6. Достоверность сообщения [Report Confidence, RC]:

– **Not Defined** – не влияет на оценку.

– **Confirmed** – имеются подробные сообщения об уязвимости.

– **Reasonable** – есть информация об уязвимости, но не ясно происхождение уязвимости.

Базовый вектор – это сокращенная запись уязвимости, в которой информация о метриках приводится вместе со значениями метрик. В скобках указываются возможные значения для указанных базовых метрик.

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

Ошибки в программном обеспечении, которые могут быть непосредственно использованы злоумышленником для реализации угроз безопасности, называют ***уязвимостями****.*

Ошибки, которые могут привести к возникновению уязвимостей – ***недостатками (слабостями) безопасности.***

CWE (Common Weakness Enumeration) – общий перечень уязвимостей и недостатков безопасности ПО, представляет собой иерархический словарь, предназначенный для разработчиков и специалистов по обеспечению безопасности ПО.

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**.

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. **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.

Таксономия системы CWE:

Для классификации недостатков используется многоуровневая структура, которая описывает древовидное устройство CWE: конечные недостатки объединяются в типы, типы – в категории, категории – в представления.

Представления:

Концепции разработки – в этом представлении CWE недостатки безопасности классифицируются с использованием принципов и понятий, которые часто встречаются при разработке ПО;

Концепции архитектуры – для анализа качества архитектурных решений на этапе проектирования;

Концепции исследований – представление, предназначенное для упрощения академических исследований. Отличается от первых двух высоким уровнем абстракций.

Type (тип):

Класс [Class, C] – слабость, которая описывается очень абстрактно, как правило, независимо от какого-либо конкретного языка или технологии. Более конкретный, чем Pillar, но более общий, чем База. Параметры: поведение, свойство и ресурс;

База [Base, B] – слабость, которая по-прежнему в основном не зависит от ресурса или технологии, но обладает достаточными деталями, чтобы предоставить конкретные методы обнаружения и предотвращения. Параметры: поведение, свойство, технология, язык и ресурс.

Вариант [Variant, V] – слабость, которая связана с определенным типом продукта, обычно с использованием определенного языка или технологии. Более конкретная, чем базовая слабость. Параметры: поведение, свойство, технология, язык и ресурс;

Pillar – слабость, которая является наиболее абстрактным типом слабости и представляет собой тему для всех слабостей класса / базы / варианта, связанных с ней.

Chain – сложный элемент, представляющий собой последовательность двух или более отдельных слабых мест, которые могут быть тесно связаны между собой в рамках программного обеспечения.

Composite – сложный элемент, состоящий из двух или более различных слабых мест, в котором все слабые места должны присутствовать одновременно, чтобы возникла потенциальная уязвимость.

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

То же самое что и CVSS, только для слабостей.

Оценка с помощью CWSS:

Метод целевой оценки – Оцениваются отдельные слабые стороны, которые обнаруживаются при проектировании или реализации конкретного («целевого») пакета программного обеспечения.

Метод обобщенной оценки – оцениваются классы слабых мест, не зависящие от какого-либо конкретного пакета программного обеспечения, в целях установления их взаимных приоритетов.

Метод контекстно-адаптированной оценки – оценки изменяются в соответствии с требованиями конкретного аналитического контекста, который может объединять приоритеты деятельности/миссии, угрозы среды, допустимый риск и т. д.

Метод агрегированной оценки – объединяются результаты нескольких оценок слабых сторон более низкого уровня и получается единая общая оценка.

Группы метрик:

Базовые [Base Finding] – охватывает внутренние риски, присущие слабому месту, доверие к точности результатов поиска, а также действенность средств контроля.

Область атаки [Attack Surface] – барьеры, которые должен преодолеть злоумышленник, для того чтобы эксплуатировать слабое место.

Среда [Environmental] – характеристики слабого места, присущие конкретной среде или операционному контексту.

БАЗОВЫЕ:

– **Техническое воздействие [Tech. Impact, TI]** – потенциальный результат, к которому может привести слабое место.

– **Приобретенная привилегия [Acquired Privilege, AP]** – тип привилегии, которую получит злоумышленник после эксплуатации слабости.

– **Уровень приобретенной привилегии [AL]**.

– **Эффективность внутреннего контроля [Internal Control Effectiveness, IC]** – способность средств контроля сделать слабое место непригодным для эксплуатации.

– **Доверие к результатам поиска [Finding Confidence, FC]** – уверенность в том, что обнаруженная проблема является слабым местом.

ОБЛАСТЬ АТАКИ:

– **Требуемая привилегия [Req. Priv., RP]** – тип привилегий, которые уже должен иметь злоумышленник, для того чтобы получить доступ к слабому месту.

– **Уровень требуемой привилегии [RL]**.

– **Вектор доступа [Access Vector, AV]** – канал, по которому злоумышленник должен обмениваться информацией, чтобы получить доступ к слабому месту.

– **Сложность аутентификации [Auth. Str., AS]** – сложность программы аутентификации, которая обеспечивает защиту кода со слабым местом.

– **Уровень взаимодействия [Level of Interaction, IN]** – действия, которые должно совершить пользователь, являющийся объектом атаки, чтобы создать условия для ее успешного осуществления.

– **Масштаб развертывания [Deployment Scope, DS]** – присутствие слабого места либо во всех развертываемых экземплярах ПО, либо ограниченно в ряде платформ и/или конфигураций.

СРЕДА:

– **Воздействие на деятельность [Business Impact, BI]** – потенциальное воздействие на деятельность в случае успешной эксплуатации слабого места.

– **Вероятность обнаружения [Likelihood of Discovery, DI]** – вероятность того, что злоумышленник может обнаружить слабое место.

– **Вероятность эксплуатации [Likelihood of Exploit, EX]** – вероятность того, что злоумышленник сможет воспользоваться слабостью.

– **Эффективность внешнего контроля [External Control Eff., EC]** – возможность контроля или смягчения последствий, которая может затруднить доступ злоумышленника к слабому месту.

– **Распространенность [Prevalence, P]** – частота появления слабого места данного типа в ПО.

4. CAPEC (Common Attack Pattern Enumeration and Classification). Шаблоны атак, классификация атак.

Цель перечня и классификации общеизвестных схем атак (CAPEC) состоит в том, чтобы обеспечить общедоступный каталог схем атак, наряду с комплексной схемой и классификационной таксономией.

CAPEC дает возможность:

1) Стандартизировать получение и описание схем атак;

2) Собирать известные схемы атак в общий перечень, который может согласованным и эффективным образом использоваться сообществом;

3) Классифицировать схемы атак, с тем чтобы пользователи могли легко определять во всем

4) Перечне то подмножество, которое подходит к их условиям;

5) С помощью явных ссылок увязать схемы атак и перечни общеизвестных слабых мест (CWE), которых такие атаки могут быть эффективными

В CAPEC используется иерархический подход. Разработано два основных **представления (механизмы атак и объекты атак).** В представлении **«механизмы атак» (Mechanisms of Attack)** шаблоны иерархически упорядочены в соответствии с механизмами, которые часто используются при эксплуатации уязвимостей. Внутри представления находятся **категории (Category)**, например **«внедрение непредвиденных элементов»**, в котором находятся **шаблон атаки метауровня (Meta Attack Pattern)**, например **«параметр внедрения»**. После метауровня следует **шаблон атаки стандартного уровня (Standard Attack Pattern)**, например **«внедрение по email»**. Самым последним звеном выступает **шаблон подробного уровня атаки.** В этом случае это **«использование метасимвола в заголовка e-mail для внедрения пейлоада»**.

1) **C (Category)** – категория представляет собой набор шаблонов атак, основанных на некоторой общей характеристике. Более конкретно, это совокупность паттернов атаки, основанная на эффекте/намерении.

2) **M (Meta Attack Pattern)** – шаблон атаки метауровня— это абстрактная характеристика конкретной методологии или техники, используемой в атаке. Шаблон мета-атаки часто лишен конкретной технологии или реализации и предназначен для обеспечения понимания высокоуровневого подхода.

3) **S (Standard Attack Pattern)** – шаблон атаки стандартного уровня в CAPEC ориентирован на конкретную методологию или технику, используемую в атаке. Это часто рассматривается как отдельная часть полностью выполненной атаки.

4) **D (Detailed Attack Pattern)** – шаблон подробного уровня атаки в CAPEC обеспечивает низкий уровень детализации, как правило, используя конкретный метод и нацеленный на конкретную технологию, и выражает полный поток выполнения.

Основная цель создания любой **таксономии** атак состоит в том, чтобы предложить такие классификационные признаки, используя которые можно наиболее точно описать классифицируемые АКС:

а) Осуществлять системное исследование вопросов защиты КС, в частности, структурировать статистические данные об атаках, выделять образцы типовых атак и делать выводы на основании собранных данных.

б) Формировать сообщения об инцидентах.

в) Разрабатывать компоненты систем защиты информации (например, подсистем обнаружения вторжений).

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

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

STIX является языком описания для обмена данными Threat Intelligence (Интеллектуальный анализ угроз безопасности) и вводит набор сущностей, а также определяет возможные типы взаимосвязей между ними. Чаще всего использует формат JSON, схемы находятся в публичном репозитории на GitHub

STIX описывает данные об угрозах как связный граф, где узлами являются **SDO (STIX Domain Objects),** то есть доменные объекты, а ребрами — **SRO (STIX Relationship objects),** как атрибутивные связи между доменными объектами.

В качестве SDO STIX определяет сущности:

1. **Схема атаки (Attack pattern)** — описывает подход (TTP), который использовал злоумышленник для взлома своей цели.

2. **Вредоносная кампания (Campaign)** — описывает последовательность вредоносных поведенческих признаков (активностей) (ограниченное время, конкретная цель)

3. **План действий (Course of action)** — описывает меры, которые нужно принять, чтобы избежать или противостоять атаке.

4. **Личность (Identity)** — описывает персоны, организации либо их группы.

5. **Индикатор (Indicator)** — описывает технические вредоносные артефакты, которые могут быть использованы для обнаружения вредоносной активности (IP-адреса, домены, хеши, ключи реестра).

6. **Intrusion set** — описывает набор поведенческих признаков и ресурсов с общими свойствами, которые, вероятней всего, подконтрольны одной организации. (продолжительное время, может иметь несколько целей)

7. **Вредоносное ПО (Malware)** — описывает экземпляры вредоносного ПО

8. **Объект наблюдения (Observed data)** — описывает не вредоносные технические артефакты.

9. **Отчет (Report)** — описывает в понятном виде какую-либо угрозу, вредоносную группировку, их TTP, жертв (аналитическая сводка, позволяющая понять суть угрозы, ее опасность, вредоносное ПО, используемые техники, тактики и процедуры, применяемые атакующей стороной)

10. **Злоумышленник (Threat actor)** — описывает персон, группы или организации, которые действуют со злым умыслом.

11. **Инструмент (Tool)** — описывает легитимное ПО, которое может быть использовано для осуществления атак (легитимный софт)

12. **Уязвимость (Vulnerability)** — описывает недостатки в требованиях, логике, дизайне, реализации ПО или железа, которые могут быть проэксплуатированы и негативно повлиять на конфиденциальность, целостность или доступность системы

В качестве SRO STIX определяет:

1. **Attributed-to –** описывает, что соответствующий злоумышленник участвует в выполнении instruction set.

2. **Targets** – описывает, что instruction set использует эксплойты соответствующей уязвимости или нацелен на тип жертв, описанный соответствующей личностью или данный шаблон атаки обычно нацелен на тип жертв или уязвимость.

3. **Uses** – описывает, что атаки, выполняемые как часть instruction set, обычно используют соответствующую схему атаки, вредоносное ПО или инструмент.

4. **Indicate** – описывает, что индикатор может обнаруживать признаки связанной кампании, instruction set или Злоумышленника.

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

OSINT (Open Source INtelligence) – разведывательная дисциплина и комплекс мероприятий, инструментов и методов для получения и анализа информации из

открытых источников. Он применяется в отношении конкретных людей, организаций, а также событий, явлений и целей.

OSINT решает задачи:

1) Сбора информации о конкурентах и поиска конкурентных преимуществ;

2) Анализа защищенности объекта, выявления уязвимых точек системы безопасности;

3) Нахождения информационных утечек;

4) Выявления возможных угроз, их источников и направленности;

5) Анализа киберпреступления (кражи данных, взломы и т.д.).

Полезными данными могут являться:

1) Регистрационные сведения о сертификате или домене сайта;

2) Персональные данные пользователей (username, email, номера телефонов);

3) Пользовательская активность в социальных сетях

4) Пользовательские запросы в поисковых системах;

5) HTML-код сайта;

6) Публичные текстовые, графические, аудио-, видеофайлы и их метаданные (например, дата, время и место создания, использованное устройство);

7) Геолокационные данные и другие виды информации

Методы бывают пассивными (с помощью сервисов и инструментов без контакта с сетью, из соц сетей, блогах, просмотр копий сайтов) и активные (с влиянием на сеть утилитами или сервисами):

1. **OSINT-фреймворк**. полная доступная база открытых источников данных. Они сгруппированы по категориям в интерактивной карте. https://osintframework.com/

2. **Shodan**. поисковая система, предназначенная для нахождения подключенных к интернету устройств по IPv4-адресам. https://www.shodan.io/

3. **Metagoofil**. метапоисковая система, которая использует другие поисковики для нахождения и извлечения находящихся в открытом доступе файлов PDF, Word, Powerpoint и Excel

4. **WHOIS**. сетевой протокол прикладного уровня, базирующийся на протоколе TCP (порт 43). Основное применение — получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем

5. **Google Dorks**. Техника для создания запросов в различных поисковых системах для обнаружения скрытой информации и уязвимостях

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

site — искать по конкретному сайту;

inurl — указать на то, что искомые слова должны быть частью адреса страницы / сайта;

intitle — оператор поиска в заголовке самой страниц;

ext или filetype — поиск файлов конкретного типа по расширению

Примеры:

inurl:"admin/default.aspx« – список адресов страниц аутентификации админов

inurl:"img/main.cgi?next_file“ – поиск ip-камер

7. Управление инцидентами информационной безопасности. The Cyber Kill Chain. Матрица ATT&CK.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – это структурированный список известных техник, приемов и тактик злоумышленников, представленный в виде таблиц.

Наборы TTP (техники, тактики и процедуры):

1) **Тактика** — как злоумышленник действует на разных этапах своей операции, какая цель или задача злоумышленника на определенным шаге (Execution — злоумышленник пытается запустить свой вредоносный код)

2) **Техника** — как злоумышленник достигает цели или поставленной задачи, какие использует инструменты, технологии, код, эксплоиты, утилиты и так далее (использование PowerShell при атаке)

3) **Процедура** — как эта техника выполняется и для чего. Например: вредоносная программа, используя PowerShell, скачивает пейлоад, который, в свою очередь, загружает Cobalt Strike для попытки запуска на удаленных хостах.

APT («развитая устойчивая угроза») – противник, обладающий современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения (например, информационных, физических и обманных).

Особенности APT-атак:

1) Направленны в отношении конкретных коммерческих организаций.

2) Объектами атаки являются весьма ограниченные целями конкретные информационные системы.

3) Эти атаки не носят массовый характер и готовятся достаточно длительный период.

4) Вредоносное ПО специально разрабатывается для конкретной атаки, чтобы штатные средства защиты, достаточно хорошо изученные злоумышленниками, не смогли обнаружить ее реализацию.

5) Целевые атаки используются для кражи информации, которую легко монетизировать, либо для нарушения доступности к критически важной информации

Cyber-Kill Chain определяет, что должны сделать злоумышленники для того, чтобы достичь своих целей, атакуя сеть, извлекая данные и поддерживая присутствие в организации.

Цепочка подразумевает следующие этапы в горизонтальном виде:

1. **Разведка**. Исследование, идентификация и выбор целевой системы для взлома.

2. **Вооружение**. Оснащение инструментами и вредоносными программами для совершения нападения.

3. **Доставка**. Донесение вредоносного контента до целевой системы.

4. **Заражение**. Запуск вредоносного кода или эксплуатация уязвимости системы.

5. **Инсталляция**. Открытие удаленного доступа и другие действия с зараженной системой.

6. **Получение управления**. Управление зараженной системой.

7. **Выполнение действий**. Сбор, кража, отправка данных, шифрование файлов, подмена и удаление данных

Затем цепочка повторяется. Как только хакер проник в сеть (за периметр), он снова начинает эту цепочку, но уже внутри сети, осуществляя дополнительную разведку и выполняя горизонтальное продвижение внутри сети. Единственный новый шаг – повышение привилегий. **Это вертикальный переход.**

Матрица ATT&CK представляет собой полное описание поведения, которое злоумышленники используют при взломе сетей, матрица полезна для различных наступательных и защитных измерений, представлений и других механизмов.

MITRE делит ATT&CK на несколько сводных матриц:

Enterprise — TTP, используемые при атаках на организации;

Mobile — TTP, связанные с переносными устройствами;

ICS — Industrial Control Systems, TTP для индустриальных систем.

В **матрице ATT&CK Enterprice** выделяют 14 тактик, которые разделены по стадиям кибератак. У каждой тактики есть техники, а у них поддетхники:

– сбор информации (reconnaissance);

– разработка ресурсов (resource development);

– первоначальный доступ (initial access);

– выполнение (execution);

– закрепление (persistence);

– повышение привилегий (privilege escalation);

– предотвращение обнаружения (defense evasion);

– получение учетных данных (credential access);

– разведка (discovery);

– перемещение внутри периметра (lateral movement);

– сбор данных (collection);

– управление и контроль (command and control);

– эксфильтрация данных (exfiltration);

– воздействие (impact)