МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ЕДЕРАЦИИ

КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ

Кафедра «Производственная безопасность и право»

ОСНОВЫ ИНФОРМАЦИОННОГО ПРАВА РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДИЧЕСКОЕ ПОСОБИЕ ДЛЯ ПОДГОТОВКИ К АККРЕДИТАЦИОННОМУ ТЕСТИРОВАНИЮ И ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Казань – 2012г.

УДК 372.8

ББК 74.5

Т66

Методическое пособие предназначено для помощи студентам в подготовке к тестированию, а так же для практических занятий в сфере основ информационного права РФ (для всех специальностей и направлений) /Сост.: ст. преп. Вахтель Р.Р., – Казань, Изд-во КГАСУ, 2012 – 44 с.

Методическое пособие для студентов в подготовке к аккредитационному тестированию, а так же для практических занятий по основам информационного права Российской Федерации.

Цель

Основной целью учебного курса **«Основы информационного права России»** является овладение информационно-правовыми компетенцией, знаниями и навыками, совершенствование общих теоретических знаний, полученных студентами в процессе изучения теории права и информатики, углубленное изучение правового регулирования информационных процессов и совершенствование навыков реферирования правовых документов, статей, книг. Необходимые теоретические знания и практические навыки, отработанные в процессе изучения учебного курса информационного права для каждого специалиста с высшим образованием служат основой профессионального роста в условиях информационного общества.

Определение понятий информационная безопасность и защита информации

Информационная безопасность:

1. состояние защищенности интересов субъектов информационных отношений;

2. состояние защищенности интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз.

Защита информации:

1. практическая реализация комплексной программы информационной безопасности;

2. процесс обеспечения информационной безопасности;

3. жестко регламентированный и динамический технологический процесс, обеспечивающий информационную безопасность.

Основные нормативные руководящие документы, касающиеся государственной тайны.

1. Конституция РФ:

Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих гос. тайну, определяется федеральным законом «О государственной тайне» (ст. 29).

2. Кодекс РФ об административных правонарушениях

Ст. 13.12 определяет ответственность за нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации, составляющей гос. тайну. Также данной статьей устанавливается наказание за использование несертифицированных ИС, баз

и банков данных, средств защиты информации, составляющей гос. тайну, если они подлежат обязательной сертификации.

Ст. 13.13 устанавливает ответственность за занятие видами деятельности в области защиты информации, составляющей гос. тайну без лицензии.

3. Уголовный кодекс РФ

Ст. 275, 276 устанавливает ответственность за выдачу гос. тайны в рамках гос. измены. Ст. 275 предусматривает освобождение от уголовной ответственности, если лицо, выдавшее гос. тайну иностранному государству, добровольно и своевременно сообщило о своем преступлении органам власти или способствовало предотвращению ущерба.

Ст. 283 устанавливает ответственность за разглашение гос. тайны, лицом, которому она была доверена или стала известна по или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены. Также определяется мера наказания за то же деяние, повлекшее по неосторожности тяжкие последствия.

Ст. 284 устанавливает ответственность за нарушение лицом, имеющим допуск к гос. тайне, правил обращения с содержащими гос. тайну документами или с предметами, сведения о которых составляют гос. тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий.

4. Патентный закон РФ

Ст. 30.2 определяет, что, если при рассмотрении в федеральном органе исполнительной власти по интеллектуальной собственности заявки на изобретение будет установлено, что содержащиеся в ней сведения составляют гос. тайну, заявка на изобретение засекречивается и считается заявкой на выдачу патента на секретное изобретение.

5. ФЗ «Об архивном деле в РФ»

Ст. 25 указывает на то, что ограничивается доступ к архивным документам, независимо от их форм собственности, содержащим гос. и иную тайну, а также к подлинникам особо ценных документов, в т.ч. уникальных документов, и документам Архивного фонда РФ, признанным находящимися в неудовлетворительном физическом состоянии.

6. Закон о государственной тайне

Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием и защитой в интересах безопасности РФ.

В законе понятие **государственная тайна** определяется как защищаемые государством сведения в области военной, внешнеполитической,

экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.

Система защиты гос. тайны – совокупность органов защиты гос. тайны, используемых ими средств, методов и мероприятий по защите сведений, составляющих гос. тайну, и их носителей.

Допуск к гос. тайне – процедура оформления права граждан на доступ к сведениям, составляющим гос.тайну, а предприятий, учреждений и организаций–на проведение работ с использованием таких сведений.

Доступ к сведениям, составляющим гос. тайну – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими гос. тайну.

Гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

Средства защиты информации - технические, криптографические, программные и др. средства для защиты сведений, составляющих гос. тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Нормативно-справочные документы и нормативно правовые акты в области защиты информации.

1. Конституция РФ:

Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения (ст.23).

2. Кодекс РФ об административных правонарушениях

Ст. 13.11 указывает на меры наказания при нарушении порядка сбора, хранения использования или распространения информации о гражданах (персональных данных).

Ст. 13.12 указывает на меры наказания при нарушении условий лицензий на осуществление деятельности в области защиты информации, в т.ч. гос. тайны. Ст. 13.13 указывает на меры наказания за занятие видами деятельности в области защиты информации, в т.ч. и составляющей гос. тайну, без лицензии.

Ст. 13.14 указывает на меры наказания за разглашение информации с ограниченным доступом лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

3. Уголовный кодекс РФ

Ст. 137 указывает на меры наказания за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, СМИ. Также устанавливается ответственность за те же деяния, совершенные лицом с использованием своего служебного положения.

Ст. 138 устанавливает ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан, а также за те же деяния, совершенные с использованием служебного положения или специальных технических средств, предназначенных для негласного получения информации. В статье 138 устанавливается ответственность за незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации.

Ст. 183 устанавливает ответственность за собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа, угроз или иным незаконным способом, а также за незаконные разглашение или использование сведений, составляющих коммерческую, налоговую, банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по работе. Также определяется ответственность за деяния подобного рода, причинившие крупный ущерб, совершенные из корыстной заинтересованности или повлекшие тяжкие последствия.

4. Гражданский кодекс РФ

Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности (ст.139).

6. Патентный закон РФ

Ст. 30.2 определяет, что, если при рассмотрении в федеральном органе исполнительной власти по интеллектуальной собственности заявки на изобретение будет установлено, что содержащиеся в ней сведения составляют гос. тайну, заявка на изобретение засекречивается и считается заявкой на выдачу патента на секретное изобретение. Засекречивание заявки,

поданной иностранными гражданами или иностранными юридическими лицами, не допускается.

Ст. 30.3 устанавливает, что сведения о секретных, содержащий гос. тайну изобретениях не публикуются в Государственном реестре изобретений РФ.

7. ФЗ «Об архивном деле в РФ»

Ст. 25

8. Закон о гос. тайне

***см.* основные нормативные руководящие документы, касающиеся государственной тайны и нормативно-справочные документы и нормативно правовые акты в области защиты информации.**

9. Закон о коммерческой тайне

Регулирует отношения, связанные с отнесением информации к ком. тайне, передачей такой информации, охраной ее конфиденциальности, определяет сведения, которые не могут составлять ком. тайну.

Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать расходов, сохранить положение на рынке или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну – научно-техническая, технологическая, производственная, финансово-экономическая и иная информация (в т.ч. секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим ком. тайны.

11. ФЗ об информации, информатизации и защите информации

12. Закон о международном информационном обмене

Целью данного закона является создание условий для участия РФ в международном информационном обмене в рамках единого мирового информационного пространства, защита интересов РФ, ее субъектов и муниципальных образований при международном информационном обмене, защита интересов, прав и свобод физических и юридических лиц при международном информационном обмене.

Объекты МИО: документированная информация, информационные ресурсы, продукты и услуги, средства МИО.

Субъекты МИО: РФ, ее субъекты, органы гос. власти и местного самоуправления, физические и юридические лица РФ и иностранных государств, лица без гражданства.

13. Закон о правовой охране программ для ЭВМ и баз данных

Закон дает определения следующим понятиям:

Программа для ЭВМ – объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

БД – объективная форма представления и организации совокупности данных (напр., статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Адаптация программы для ЭВМ или БД – внесение изменений в целях обеспечения функционирования программы для ЭВМ или БД на конкретных технических средствах или под управлением конкретных программ.

Модификация (переработка) программы для ЭВМ или БД – любые их изменения, не являющиеся адаптацией.

Декомпилирование программы для ЭВМ – технический прием, включающий преобразование объектного кода в исходный текст в целях изучения структуры и кодирования программы для ЭВМ.

Воспроизведение программы для ЭВМ или БД – изготовление одного или более экземпляров программы для ЭВМ или БД в любой материальной форме, а также их запись в память ЭВМ.

Распространение программы для ЭВМ или БД – предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ или БД, в т.ч. сетевыми и иными способами, путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей.

Выпуск в свет (опубликование) программы для ЭВМ или БД – предоставление экземпляров программы для ЭВМ или БД с согласия автора неопределенному кругу лиц (в т.ч. путем записи в память ЭВМ и выпуска печатного текста), при условии, что количество таких экземпляров должно удовлетворять потребности этого круга лиц, принимая во внимание характер указанных произведений.

Использование программы для ЭВМ или БД – выпуск в свет, воспроизведение, распространение и иные действия по их введению в хозяйственный оборот (в т.ч. в модифицированной форме).

Правообладатель – автор, его наследник, а также любое физическое или юридическое лицо, которое обладает исключительным правом на программу для ЭВМ или БД в силу закона или договора.

14. Закон о СМИ

15. Закон о рекламе

16. Закон о товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров

17. Закон об ЭЦП

18. Закон о банках и банковской деятельности

Банк обязывается хранить тайну об операциях по счету и вкладу и др. информацию, относящуюся к клиентам, независимо от того имеет эта информация действующую или потенциальную коммерческую ценность или нет.

19. Закон об основах муниципальной службы в РФ

20. Федеральный закон о связи

21. ГОСТ – Р – 50922 – 96 «Защита информации. Основные термины и определения».

22. Указ Президента РФ «О мерах по обеспечению ИБ РФ в сфере МИО»

Федеральная служба охраны РФ должна обеспечивать поддержание и развитие сегмента сети Интернет для федеральных органов гос. власти и субъектов РФ. Запрещено включение ИС, сетей и ПК, в которых обрабатывается информация, содержащая гос. тайну в сеть Интернет.

Вопросы авторских и смежных прав

Данные вопросы регулируются в законе об авторских и смежных правах. Закон регулирует отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания (смежные права).

Под автором понимается физическое лицо, творческим трудом которого создано произведение.

Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от

назначения и достоинства произведения, а также от способа его выражения. Авторское право распространяется на обнародованные и на необнародованные произведения, существующие в письменной, устной форме, форме звуко- или видеозаписи, изображения, объемно-пространственной (скульптура, макет) и в др. формах. Передача прав на материальный объект не влечет передачи авторских прав на произведение, выраженное в этом объекте.

Объектами авторского права являются:

- литературные произведения (включая программы для ЭВМ);

- драматические и музыкально-драматические произведения, сценарные произведения;

- хореографические произведения и пантомимы;

- музыкальные произведения с текстом или без текста;

- аудиовизуальные произведения (кино- и телепроизведения);

- произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и др. произведения изобразительного искусства;

- произведения декоративно-прикладного и сценографического искусства;

- произведения архитектуры, градостроительства и садово-паркового искусства;

- фотографические произведения;

- географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и к другим наукам.

Охрана программ для ЭВМ распространяется на все виды программ для ЭВМ (в т.ч. на ОС), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код.

К объектам авторского права также относятся: производные произведения (переводы, обработки, аннотации, рефераты, резюме, обзоры и т.п.); сборники (энциклопедии, антологии, БД).

Не являются объектами авторского права:

- официальные документы (законы, судебные решения и т.п.), их официальные переводы;

- гос. символы и знаки (флаги, гербы, ордена, денежные знаки);

- произведения народного творчества;

- сообщения о событиях и фактах, имеющие информационный характер.

Авторские права делятся на 2 группы: личные неимущественные и имущественные. Личные неимущественные права неразрывно связаны с личностью автора и не могут быть переданы. К ним относят:

1) Право авторства – право признаваться автором произведения;

2) Право на имя – право использовать произведение под своим именем, псевдонимом или анонимно;

3) Право на защиту репутации автора – право на защиту произведения от искажения или иного посягательства, способного принести ущерб чести и достоинству автора.

4) Право на обнародование – обеспечение доступа третьих лиц к произведению

К имущественным правам относятся:

1) Право на воспроизведение (запись с одного носителя на другой, копирование)

2) Право на распространение экземпляров произведений любым способом (продажа, сдача в прокат и др.)

3) Право на публичный показ, исполнение и передачу в эфир произведений

4) Право на перевод и переработку

5) Право на доведение до общего сведения, в т.ч. в сети Интернет.

Закон о защите авторских прав предусматривает общий срок охраны авторских прав и ряд специальных. По общему правилу авторские права охраняются в течении жизни автора и 70 лет после его смерти. Личные неимущественные права охраняются бессрочно. Специальные сроки охраны авторских прав:

- при соавторстве срок охраны составляет 70 лет после смерти последнего соавтора;

- при опубликовании произведения после смерти автора оно охраняется 70 лет после опубликования;

- срок охраны программ для ЭВМ и БД составляет 50 лет после смерти автора.

По окончании срока охраны произведение переходит в разряд общественного достояния.

Имущественные права могут передаваться только по авторскому договору. В нем указываются:

1) Виды и объем передаваемых имущественных прав. Все права, не переданные по авторскому договору сохраняются за автором.

2) Условия о сроке и территории распространения авторских прав. В случае отсутствия срока в договоре он считается заключенным на 5 лет. Если не указана территория, договор действует по всей РФ.

3) Размер и порядок выплаты авторского вознаграждения.

4) Другие условия, которые определяют стороны договора.

Авторский договор должен быть заключен в письменной форме. Существует несколько видов авторских договоров: авторский договор заказа (автору дается задание на создание произведения), исключительный договор (передаются все имущественные права), неисключительный договор (передается часть имущественных прав), краткосрочные (до года), среднесрочные и долгосрочные (свыше 5 л.) договоры.

За нарушение авторских прав устанавливается гражданско-правовая, административная и уголовная ответственность (гражданско-правовая – в случае нарушения исключительных прав, административная и уголовная – за плагиат).

Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Место информационной безопасности экономических систем в национальной безопасности страны.

Задачами в сфере обеспечения информационной безопасности РФ являются:

1) разработка основных направлений гос. политики в области обеспечения информационной безопасности РФ, а также мероприятий и механизмов, связанных с реализацией этой политики;

2) развитие и совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности РФ, а также системы противодействия этим угрозам;

3) разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности РФ, а также сертификации этих систем и средств;

4) совершенствование нормативной правовой базы в области информационной безопасности РФ;

5) установление ответственности должностных, юридических лиц и граждан за несоблюдение требований информационной безопасности;

6) координация деятельности органов гос. власти, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности РФ;

7) разработка методов повышения эффективности участия государства в формировании информационной политики государственных средств массовой информации;

8) обеспечение технологической независимости РФ в областях информатизации, определяющих ее безопасность, а также в области создания специализированной военной вычислительной техники;

9) разработка современных методов и средств защиты информации, прежде всего для систем управления войсками и оружием, экологически опасными и экономически важными производствами;

10) развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;

11) взаимодействие с международными и зарубежными организациями при решении вопросов обеспечения безопасности информации, передаваемой с помощью международных систем связи;

12) обеспечение условий для развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;

13) создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

Особенности обеспечения информационной безопасности РФ в сфере экономики. Согласно доктрине оба ИБ обеспечение информационной безопасности РФ в сфере экономики играет ключевую роль в обеспечении национальной безопасности РФ.

Воздействию угроз информационной безопасности в сфере экономики наиболее подвержены:

- система государственной статистики;

- кредитно - финансовая система;

- информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;

- системы бухгалтерского учета предприятий, учреждений и организаций;

- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, предприятий, организаций.

Недостаточный контроль деятельности отечественных и зарубежных структур, занимающихся созданием и защитой систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает угрозу безопасности России в экономической сфере. Бесконтрольное привлечение иностранных фирм к созданию подобных систем создает благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации со стороны иностранных спецслужб.

Широкое использование импортных средств информатизации создает угрозу возникновения технологической зависимости России от иностранных государств. Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением в компьютерные системы и сети банков и иных кредитных организаций.

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. Экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения коммерческой тайны. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней.

Основными мерами по обеспечению информационной безопасности РФ в сфере экономики являются:

- гос. контроль за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации;

- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи экономической информации;

- разработка и внедрение национальных систем электронных платежей, систем электронных денег и электронной торговли, стандартизация этих

систем, а также разработка нормативной правовой базы, регламентирующей их использование;

- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;

- совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

Три аспекта информационной безопасности: доступность, целостность, конфиденциальность. Три вида возможных нарушений информационной системы.

Доступность – возможность получения информации за приемлемое время лицами, процессами или системами, имеющими на это право.

Считается, что доступность информации является важнейшим элементом информационной безопасности: ИС создаются для получения информационных услуг, а если предоставить услуги пользователям становится невозможно, это наносит ущерб всем субъектам информационных отношений.

Целостность – актуальность и непротиворечивость информации, защищенность от разрушения и несанкционированного изменения.

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля динамической целостности применяются при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Конфиденциальность – защищенность от несанкционированного доступа к информации.

Аспект конфиденциальность считается наиболее проработанным в РФ

Существует 3 вида возможных нарушений ИС: нарушение целостности, доступности и конфиденциальности информации.

Нарушения доступности информации могут быть связаны со следующими факторами: отказы пользователей, внутренние отказы, отказ поддерживающей инфраструктуры. К отказам пользователей относятся: нежелание работать в силу несоответствия запросов пользователей с фактическими характеристиками системы и по др. причинам, невозможность работать в силу отсутствия соответствующей подготовки или отсутствия технической поддержки. Основными источниками внутренних отказов являются: случайное или умышленное отступление от правил эксплуатации,

ошибки при (пере)конфигурировании системы, отказы программного и аппаратного обеспечения, разрушение данных, разрушение или повреждение аппаратуры. Отказы поддерживающей инфраструктуры предполагают случайное или умышленное нарушение работы систем связи, электропитания, тепло и водоснабжения; разрушение или повреждение помещений и т.п.

Нарушения целостности информации предполагают нарушение статической и динамической целостности. Статическая целостность может быть нарушена путем ввода неверных данных или изменения данных. Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочивание, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Конфиденциальность данных может быть **нарушена** путем перехвата данных (передаваемых в разговоре, в письме, по сети), атак (в т.ч. подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), методы морально-психологического воздействия (напр., маскарад - выполнение действий под видом лица, обладающего полномочиями для доступа к данным). Также конфиденциальность информации может быть нарушена в результате злоупотребления полномочиями (напр., системный администратор способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д.).

Понятие угрозы. Классификация угроз.

Угроза ИБ – единичное или комплексное, реальное или потенциальное, активное или пассивное проявление возможностей источников угрозы создавать неблагоприятные события, оказывающие дестабилизирующее воздействие на защищаемую информацию (информационный ресурс).

Угроза ИБ – потенциальная возможность нарушения ИБ.

Источники угрозы:

1. Люди: злоумышленно или непреднамеренно.

2. Случайные факторы (окружающая среда: природные, антропогенные факторы).

Атака – 1. попытка реализации угрозы; 2. попытка нарушения ИБ.

Тот, кто предпринимает попытку реализации угрозы, называется **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы**.

Окно опасности – промежуток времени от момента возникновения угрозы до момента ее ликвидации. Пока существует окно опасности, возможны успешные атаки на ИС.

Классификация угроз.

1. По источнику воздействия:

- внешние;

- внутренние.

Внешние угрозы в свою очередь подразделяются на случайные (со стороны природной среды) и целенаправленные (со стороны противников). Внутренние угрозы также могут быть случайными и целенаправленными (персонал). Случайные внутренние угрозы подразделяются на ошибки персонала, аппаратные отказы и сбои, программные отказы.

2. По результату воздействия:

- нарушение целостности;

- нарушение доступности;

- нарушение конфиденциальности.

3. По условию начала осуществления воздействия:

- атака по запросу от атакуемого объекта;

- атака по наступлению ожидаемого события;

- безусловная атака.

4. По величине принесенного ущерба:

- предельный, после которого фирма может стать банкротом;

- значительный, но не приводящий к банкротству;

- незначительный, который фирма за какое-то время может компенсировать.

5. По характеру несанкционированного доступа:

- непосредственный (подразделяется по уровням: внешней среды, уровень абонентов сети, уровень общих сетевых средств (локальная машина);

- опосредованный: съем электромагнитных излучений, кража (печатные и магнитные материальные носители), внутренне разрушение программных средств (объекты воздействия: внешние и внутренние каналы связи, удаленные терминалы, отдельные АРМы, системны и прикладные программные файлы и БД).

Классификация потенциальных нарушителей информационной безопасности.

Существуют следующие возможные типы нарушителей в системе:

1. **«Неопытный пользователь»** - сотрудник, зарегистрированный как пользователь системы, который может предпринимать попытки выполнения запрещенных операций, доступа к защищаемым ресурсам КИС с превышением своих полномочий, ввода некорректных данных. Его действия могут совершаться по ошибке, некомпетентности или халатности без злого умысла, при этом обычно используются только штатные (доступные сотруднику) аппаратные и программные средства.

2. **«Любитель»** - сотрудник, зарегистрированный как пользователь системы, пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из «спортивного интереса». Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей и т.п. других пользователей), недостатки в построении системы защиты и доступные ему штатные (установленные на рабочей станции) программы. То есть данный тип нарушителя выполняет несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств. Он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства (отладчики, служебные утилиты), самостоятельно разработанные программы или стандартные дополнительные технические средства.

3. **«Мошенник»** - сотрудник, зарегистрированный как пользователь системы, который может предпринимать попытки выполнения незаконных вторжений в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные (установленные на рабочей станции и доступные ему) аппаратные и программные средства от своего имени или от имени другого сотрудника (зная его имя и пароль, используя его кратковременное отсутствие на рабочем месте и т.п.).

4. **«Внешний нарушитель (злоумышленник)»** - постороннее для организации лицо, действующее целенаправленно из корыстных интересов, мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома систем защиты, характерных для сетей общего пользования (в особенности сетей на основе IP-протокола), включая удаленное внедрение программных закладок и использование специальных инструментальных и технологических программ, используя имеющиеся слабости протоколов обмена и системы защиты узлов сети КИС. К категории внешних нарушителей могут

относиться уволенные сотрудники, клиенты, поставщики, члены преступных организаций.

5. **«Внутренний злоумышленник»** - сотрудник, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных интересов или мести, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы получения реквизитов доступа, пассивные средства (технические средства перехвата без модификации компонентов системы), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий как изнутри, так и извне - из сетей общего пользования. К категории внутренних злоумышленников могут относится зарегистрированные пользователи КИС (сотрудники); сотрудники других организаций, допущенные к работе с КИС; технический персона, обслуживающий здания; сотрудники службы безопасности.

Пользователи и обслуживающий персонал из числа сотрудников организации имеют наиболее широкие возможности по осуществлению несанкционированных действий, т.к. имеют доступ к ресурсам и хорошие знания технологии обработки информации и защитных мер в организации. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа.

Криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников организации всеми доступными силами и средствами.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в КИС. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными сотрудниками организации и криминальными структурами.

Организации, занимающиеся разработкой, поставкой и ремонтом оборудования, информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Криминальные структуры могут использовать эти организации с целью доступа к защищаемой информации в КИС.

Составление портрета нарушителя информационной безопасности (описать технологию, какие пункты должны быть описаны в портрете нарушителя).

Построение модели злоумышленника предполагает выполнение следующих действий:

1. Определение типа злоумышленника (конкурент, сотрудник компании, клиент и т.д.).

2. Определение положения злоумышленника по отношению к объектам защиты (внутренний, внешний).

3. Определение уровня знаний злоумышленника об объектах защиты и окружении (высокий, средний, низкий).

4. Определение уровня возможностей по доступу к объектам защиты (максимальные, средние, минимальные).

5. Определение времени совершения нарушения (постоянно, в определенные временные интервалы).

6. Определение наиболее вероятного местоположения злоумышленника во время реализации атаки.

Присвоив перечисленным параметрам модели злоумышленника качественные значения, можно определить потенциал злоумышленника, т.е. интегральную характеристику возможностей злоумышленника по реализации угроз.

Способы нарушений информационной безопасности и меры противодействия им (то есть каким образом угрозы могут реализоваться).

Под нарушением информационной безопасности понимается любой вид компрометации каких-либо аспектов безопасности систем и/или сетей, к их числу относятся:

- ✓ потеря конфиденциальности информации;
- ✓ нарушение целостности информации;
- ✓ нарушение доступности информационных услуг;
- ✓ неправомочное использование услуг, систем или информации;
- ✓ повреждение систем.

Международные стандарты информационного права.

Существует 2 вида стандартов и спецификаций:

- **оценочные** стандарты для классификации ИС и средств защиты по требованиям безопасности;

- **технические** спецификации, регламентирующих различные аспекты реализации средств защиты.

Оценочные стандарты играют роль архитектурных спецификаций. Технические спецификации определяют, как строить ИС предписанной архитектуры.

Доверенная система определяется как «система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа». Следует отметить, что «Оранжевая книга» рассматривает вопросы целостности и конфиденциальности, вопросы доступности не затрагиваются.

Степень доверия оценивается по 2 основным критериям:

1. **Политика безопасности** - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Чем выше степень доверия к системе, тем строже и многообразнее должна быть политика безопасности. Это активный аспект защиты, включающий анализ возможных угроз и выбор мер противодействия.

2. **Уровень гарантированности** - мера доверия, которая может быть оказана архитектуре и реализации ИС. Уровень гарантированности показывает, насколько корректны механизмы реализации политики безопасности. Это пассивный аспект защиты.

Монитор обращений должен обладать тремя качествами:

1. Изолированность (возможность отслеживания работы монитора).

2. Полнота (должен вызываться при каждом обращении, не должно быть способов обойти его)

3. Верифицируемость (должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования).

Произвольное управление доступом - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность состоит в том, что лицо (обычно владелец объекта) может предоставлять (или отбирать) другим субъектам права доступа к объекту.

Безопасность повторного использования объектов - дополнение к средствам управления доступом, предохраняющее от случайного или

преднамеренного извлечения конфиденциальной информации из «мусора». Должна гарантироваться для областей оперативной памяти (буферов с образами экрана, расшифрованными паролями и т.п.), дисковых блоков и магнитных носителей в целом.

Для реализации **принудительного управления доступом** с субъектами и объектами ассоциируются **метки безопасности**. Метка субъекта описывает его благонадежность, метка объекта - степень конфиденциальности содержащейся в нем информации. Метки состоят из двух частей - уровня секретности и списка категорий. Назначение списка категорий - описать предметную область, к которой относятся данные.

Принудительное (или мандатное) управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Субъект получает полный доступ к объекту, только если их метки совпадают. Субъект получает доступ только на чтение, если его метка имеет больший уровень привилегий, чем метка объекта. Субъект может записывать информацию в объект, если его метка безопасности меньше метки объекта. Описанный способ управления доступом называется принудительным, т.к. он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

1) **Аутентификация:** обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и периодически во время сеанса. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

2) **Управление доступом:** защита от несанкционированного использования ресурсов, доступных по сети.

3) **Конфиденциальность данных:** защита от несанкционированного получения информации.

4) **Целостность данных:** подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением соединения или без, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

5) **Неотказуемость** (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника.

«Общие критерии» содержат два основных вида требований безопасности:

- функциональные – активный аспект защиты;

Сгруппированы на основе выполняемой роли или обслуживаемой цели безопасности. Всего 11 функциональных классов (некоторые: идентификация и аутентификация; защита данных пользователя; управление безопасностью – атрибутами и параметрами безопасности; аудит безопасности; приватность – защита пользователя от раскрытия и несанкционированного использования его идентификационных данных; криптографическая поддержка).

- требования доверия – пассивный аспект.

Введено 10 классов требований доверия (некоторые: разработка, поддержка ЖЦ, тестирование, оценка уязвимостей, поставка и эксплуатация, управление конфигурацией, руководства – требования к документации и т.д.). Также в ОК определяются 7 оценочных уровней доверия.

Профиль защиты представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (напр., ОС в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Недостатки ОК. Отсутствие объектного подхода (функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование). Отсутствуют архитектурные требования.

Также в стандарте определяются требования, которым нужно следовать для обеспечения безопасности информации.

Виды защиты информации.

1. правовая защита информации (нормативно-правовые акты и т.д.);
2. организационная защита информации (документы, персонал, режим работы и т.д.)
3. инженерно-техническая защита информации (от «жучков», утечки по каналам связи)
4. программная
5. аппаратная
6. криптографическая
7. комплексная

А. Правовая защита. К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования. Также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

Б. Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно – правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности

К организационным мероприятиям можно отнести:

- *Организацию режима и охраны*. Их цель- исключение возможности тайного проникновения на территорию и в помещение посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержания надежного пропускного режима и контроля сотрудников и посетителей и др.;
- *Организацию работы с сотрудниками*, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- *Организацию работы с документами и документированной информацией*, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение.

• *Организацию использования технических средств* сбора, обработки накопления и хранения конфиденциальной информации.

• *Организацию работу по анализу внутренних и внешних угроз* конфиденциальной информации и выработке мер ее защиты.

• *Организацию работы по проведению систематического контроля за работой персонала* с конфиденциальной информацией порядком учета, хранения документов и технических носителей.

Одним из важнейших организационных мероприятий является создание специальных штатных служб защиты информации в закрытых информационных системах в виде администратора безопасности сети и администратора распределенных баз и банков данных, содержащих сведения конфиденциального характера

Организационные меры являются решающим звеном формирования и реализации комплексной защиты информации и создания системы безопасности предприятия.

В. Инженерно-техническая защита – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации

Г. программные средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки, хранения, накопления и передачи, сбора данных.

Д. Аппаратные средства

Сюда входят приборы, устройства, приспособления и другие технические решения

Основная задача аппаратных средств – обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности.

Е. Криптографические средства – это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Ж. Комплексные средства

Совокупная реализация программных и аппаратных средств и криптографических методов защиты информации.

Организационная защита информации (ОРГАНИЗАЦИЯ работы с информацией – люди, бумаги, документопотоки).

Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно – правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности

К организационным мероприятиям можно отнести:

- *Организацию режима и охраны*. Их цель - исключение возможности тайного проникновения на территорию и в помещение посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержания надежного пропускного режима и контроля сотрудников и посетителей и др.;
- *Организацию работы с сотрудниками*, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- *Организацию работы с документами и документированной информацией*, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение.
- *Организацию использования технических средств* сбора, обработки накопления и хранения конфиденциальной информации.
- *Организацию работу по анализу внутренних и внешних угроз* конфиденциальной информации и выработке мер ее защиты.
- *Организацию работы по проведению систематического контроля за работой персонала* с конфиденциальной информацией порядком учета, хранения документов и технических носителей.

Одним из важнейших организационных мероприятий является создание специальных штатных служб защиты информации в закрытых информационных системах в виде администратора безопасности сети и администратора распределенных баз и банков данных, содержащих сведения конфиденциального характера

Организационные меры являются решающим звеном формирования и реализации комплексной защиты информации и создания системы безопасности предприятия.

Организационные средства защиты ПЭВМ и информационных сетей применяются:

- При проектировании, строительстве и оборудовании помещений, узлов сети и других объектов информационной системы, исключающих влияние стихийных бедствий, возможность недозволенного проникновения в помещения и др.;

- При подборе и подготовке персонала. В этом случае предусматриваются проверка принимаемых на работу, создание условий, при которых персонал был бы заинтересован в сохранности данных, обучение правилам работы с закрытой информацией, ознакомление с мерами ответственности за нарушение правил защиты и др.;

- При хранении и использовании документов и других носителей (маркировка, регистрация, определение правил выдачи и возвращения, ведение документации и др.);

- При соблюдении надежного пропускного режима к техническим средствам, к ПЭВМ и информационным системам при сменной работе (выделение ответственных за защиту информации в сменах, контроль за работой персонала, ведение (возможно и автоматизированное) журналов работы, уничтожение в установленном порядке закрытых производственных документов);

- При внесении изменений в программное обеспечение (строгое санкционирование, рассмотрение и утверждение проектов изменений, проверка их на удовлетворение требованиям защиты, документальное оформление изменений и др.);

- При подготовке и контроле работы пользователей.

Ответы на тестовые вопросы.

1. Общие положения об информации ограниченного доступа закреплены:

в ФЗ «Об информации, информационных технологиях и защите информации»;

2. Административные дела в сфере нарушений требований защиты информации, составляющей государственную тайну, рассматривает:

Федеральная служа безопасности;

3. Размер компенсации за незаконное использование объектов авторского права составляет:

от 10.000 до 5.000.000 рублей;

4. Российский закон «Об авторском праве и смежных правах» предполагает, что исключительные права на использование служебных произведений принадлежат:

работодателю, если иное не предусмотрено в договоре между ним и автором;

5. К объектам информационных правоотношений относится:

информация и связанные с ней объекты;

7. Компьютерные преступления относятся к компетенции:

так или иначе, все органы правомочны расследовать те или иные компьютерные преступления;

8. Может ли соавтор использовать произведение, созданное им в со-авторстве, без согласия другого соавтора?

при раздельном соавторстве может, при нераздельном только с согласия соавтора;

9. Ответственность за проведение в организации мероприятий по защите коммерческой тайны несет:

генеральный директор;

10. Право собственности в РФ не может быть установлено в отношении:

любой информации;

11. Право на авторство является:

личным неимущественным правом автора;

12. Авторское право на литературное произведение возникает:

с момента его создания;

13. Доменное имя по правой природе можно отнести:

средству индивидуализации информационного ресурса;

14. Информационное право – это:

совокупность правовых норм, регулирующих отношения по поводу создания, получения, использования и распространения информации и вязанных с ней информационных объектов;

15. Время хранения документов в Архивном фонде РФ устанавливается:

определено указом Президента РФ, а в отношении архивных документов силовых ведомств данными органами**;**

16. Программы для ЭВМ охраняются в Российской Федерации как:

как объекты авторского права – литературные произведения;

17. Информации как объекту правоотношений не свойственны следующие признаки:

количественная неопределенность;

физический износ;

18. Обладатели коммерческой тайны обязаны представить сведения, составляющие коммерческую тайну органам государственной власти:

по их мотивированному законному требованию;

19. Может ли охраняться авторским правом название произведения?

да, но при условии, что оно представляет собой результат творческой деятельности;

20. Обладателем коммерческой тайны не может быть:

юрисконсульт В.А. Иванов;

21. Информация ограниченного доступа – это:

информация, доступ к которой ограничен в силу федерального закона;

22. К информации ограниченного доступа не относится:

санитарно-эпидемиологическая информация;

23. Ограничивается вывоз следующей документированной информации:

информация, относящаяся к персональным данным работника;

информация о факте разработки нового вида компьютерного вируса.

24. Лицензирование в сфере технической защиты конфиденциальной информации осуществляет:

ФСТЭК (Федеральная служба по техническому и экспортному контролю);

25. Какой орган государственной власти осуществляет координацию органов власти по вопросам реализации федерального законодательства о государственной тайне

Межведомственная комиссия по защите государственной тайны;

26. Базовым законом, регулирующим информационные отношения является:

ФЗ «Об информации, информационных технологиях и защите информации»;

27. Использование архивных документов в коммерческих целях допускается:

в зависимости от вида архивного фонда и вида (категории) архивного документа и только на основании лицензионного соглашения;

28. Авторское право в России действует в течение жизни автора и:

70 лет после его смерти;

29. Общественным достоянием являются следующие произведения:

произведения, на которые истек срок действия авторского права;

30. Убытки, причиненные в результате отзыва автором произведения, пользователю возмещает:

автор;

31. В отношении допуска к каким сведениям, составляющих государственную тайну, не проводятся проверочные мероприятия:

секретных сведений;

32. Автором аудиовизуального произведения является:

режиссер-постановщик, автор сценария и автор музыкального произведения, специально созданного для этого аудиовизуального произведения;

33. Работник по окончании трудовых отношений обязан не разглашать коммерческую тайну в течении:

в течении 3 лет с момента трудоустройства в другом месте;

34. Количество передаваемых обязательных экземпляров документов определяется:

государством, но по его требованию и за счет получателя может варьироваться;

35. Индивидуальный предприниматель при защите коммерческой тайне во всех случаях обязан:

размещать на документах гриф «Коммерческая тайна»;

36. Ноу-хау является:

разновидностью информации, составляющей коммерческую тайну;

37. К числу обязательных мер охраны коммерческой тайны относятся:

организационные меры;

38. Интернет-право по общепризнанной точке зрения является:

подотраслью (институтом) информационного права;

39. За незаконное разглашение сведений, составляющих коммерческую тайну, может наступать:

административная, дисциплинарная и гражданско-правовая ответственность;

40. Срок действия авторских прав на произведение, созданное в результате соавторства, исчисляется следующим образом:

авторское право действует в течение всей жизни и 70 лет после смерти последнего автора, пережившего других соавторов;

41. Общий срок охраны государственной тайны составляет:

30 лет.

42. Право авторства охраняется в течение:

бессрочно;

43. «Контрафактный экземпляр произведения» – это:

копия, изготовление и использование которой влечет нарушение исключительных прав;

44. Охраняются ли в Российской Федерации фотографические произведения?

да;

45. К личному неимущественному праву автора относится:

право на имя;

46. Авторское право охраняет:

форму произведения;

47. Исчисление срока охраны авторских прав начинается:

с 1 января года, следующего за годом, в течение которого имел место юридический факт, послуживший основанием для начала течения срока;

48. Какие из произведений не охраняются авторским правом в Российской Федерации?

произведения народного творчества;

49. Ответственность за компьютерные преступления устанавливается:

главой 28 Уголовного кодекса РФ;

50. Рассмотрение информации в качестве сведений является отражением:

семантического подхода к информации.

Тесты:

1. Защищаемые банками сведения о вкладах и счетах своих клиентов, банковских операциях по счетам и сделках в интересах клиента, относятся к тайне:

- государственной

- личной

- банковской

- коммерческой

2. Утрата документов, содержащих государственную тайну - это...:

- злоупотребление должностным положением

- выход документов, содержащих государственную тайну, из владения лица, имеющего допуск к государственной тайне

- получение взятки

- служебный подлог

3. Осуществлением единой государственной политики в области засекречивания сведении занимается...:

- правительство Российской Федерации

- органы исполнительной власти Российской Федерации

- парламент Российской Федерации

- межведомственная комиссия по защите государственной тайны

4. Совокупность категории сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральный законодательством, составляют…:

- перечень документов с грифом секретности

- перечень сведений, составляющих государственную тайну

- документы общего учета

- перечень документов, относящихся к служебной тайне

5. Неправомерный доступ к информации - это...:

- самовольное получение информации без разрешения ее собственника или владельца

- продажа информации по инициативе владельца

- аренда информации пользователем

- покупка информации с разрешения собственника

6. Защита компьютерной информации введена...:

- Уголовным кодексом Российской Федерации

- Гражданским кодексом Российской Федерации

- Конституцией Российской Федерации

- Семейным кодексом РФ

7. Информационная безопасность - это...:

- установленная законом процедура доступа к соответствующим сведениям и ответственность за разглашение этих сведений

- защищаемая законом конфиденциальная информация, ставшая известной в государственных органах

- определенный порядок реализации полномочии различных субъектов в области производства

- состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз

8. Государственная измена-это...:

- организации массовых беспорядков

- получение сведений от представителей иностранных государств

- посягательство на суверенитет государства

- умышленное сообщение иностранному государству гражданином Российской Федерации сведений, составляющих государственную тайну

9. К способам неправомерного доступа к информации относится…:

- разрешение владельца на доступ к информации

- доступ к компьютеру с разрешения собственника

представление фиктивных документов на право доступа к информации

пользование информацией с разрешения собственника

10. Степень секретности сведений, составляющих государственную тайну, должна соответствовать…

- тяжести ущерба, который может быть нанесен безопасности Российской Федерации

- тяжести возможного морального вреда

- предусмотренной уголовной ответственности

- упущенной выгоде

11. Гриф секретности – это…

- данные Правительства Российской Федерации

- данные о документе

- реквизиты, свидетельствующие о степени секретности сведений

- данные об авторе документа

12. Перечень сведений, составляющих государственную тайну утверждается…:

- указом Президента РФ

- федеральным законом

- постановлением правительства РФ

- межведомственной комиссией

13. Общее направление защиты от иностранных технических разведок и ее утечки по техническим каналам связи формирует….:

- федеральная служба по техническому и экспортному контролю

- служба внешней разведки РФ

- президент РФ

- федеральная служба безопасности РФ

14. Служебные сведения, доступ к которым ограничен органами государственной власти, именуется…:

- служебной тайной

- коммерческой тайной

- медицинской тайной

- тайной следствия

15. Система правовых, организационных, технических и иных мер, предпринимаемых обладателем коммерческой тайны и конфидентом коммерческой тайны по обеспечению ограниченного доступа к соответствующей информации, именуется…:

- режимом коммерческой тайны

- грифом секретности

- государственной тайны

- служебной тайны

16. В случае причинение вреда в результате распространения сведений, порочащих честь и достоинство, деловую репутацию, осуществляется…:

- компенсация морального вреда
- подача гражданского иска
- уголовное преследование
- привлечение к административной ответственности

17. Не подлежат отнесению к государственной тайне и засекречиванию сведения о ….:

- о размерах золотого запаса
- содержании стратегических и оперативных планов
- силах и средствах гражданской обороны
- финансовой или денежно-кредитной деятельности

18. Если информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет доступа на законном основании, то она называется….:

- коммерческой тайной
- конфиденциальной информацией
- государственной тайной
- документированной информацией

19. Федеральный орган исполнительной власти, уполномоченный в области обеспечения информационной безопасности, именуется ….:

- федеральной службой безопасности
- министерством внутренних дел РФ
- правительством РФ
- администрацией муниципального образования

20. Правовой базой сохранения нотариальной тайны является…:

- конституция РФ
- закон РФ «О государственной тайне»
- федеральный закон «О банках и банковской деятельности»
- гражданский кодекс

21. Не является основанием для отказа гражданину в допуске к государственной тайне…:

- его временная нетрудоспособность
- признание судом гражданина недееспособным
- признание его особо опасным рецидивистом
- наличие у гражданина судимости

22. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, именуется…:

- обладателем информации
- распространителем информации
- информационным агентом
- специалистом

23. Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, представляет собой ….:

- информационно-телекоммуникационную сеть
- электронное сообщение
- конфиденциальную информацию
- распространение информации

24. Возможность получения информации и ее использования именуется _____ информации:

- доступом к
- конфиденциальностью
- оперативностью
- распространением

25. Безопасность учреждений РФ, находящихся за пределами ее территории, и командированных за границу граждан РФ, имеющих допуск к государственной тайне, осуществляет…:

- служба внешней разведки РФ
- министерство внутренних дел РФ
- министерство иностранных дел
- федеральная миграционная служба

Ответы на тесты:

1. банковской

2. выход документов, содержащих государственную тайну, из владения лица, имеющего допуск к государственной тайне

3. Правительство Российской Федерации

4. перечень сведений, составляющих государственную тайну

5. самовольное получение информации без разрешения ее собственника или владельца

6. Гражданским кодексом Российской Федерации

7. установленная законом процедура доступа к соответствующим сведениям и ответственность за разглашение этих сведений

8. умышленное сообщение иностранному государству гражданином Российской Федерации сведений, составляющих государственную тайну

9. представление фиктивных документов на право доступа к информации

10. тяжести ущерба, который может быть нанесен безопасности Российской Федерации

11. реквизиты, свидетельствующие о степени секретности сведений

12. указом Президента РФ

13. федеральная служба по техническому и экспортному контролю

14. служебной тайной

15. режимом коммерческой тайны

16. компенсация морального вреда

17. о размерах золотого запаса

18. коммерческой тайной

19. федеральной службой безопасности

20. конституция РФ

21. его временная нетрудоспособность

22. обладателем информации

23. информационно-телекоммуникационную сеть

24. доступом к

25. служба внешней разведки РФ

Задачи

1. Правовое агентство «Велес» обратилось в департамент ценных бумаг ЦБ РФ с просьбой предоставить ему право на распоряжение информации о ценных бумагах коммерческих банков и других кредитных организаций. Руководство департамента, рассмотрев заявление и нотариально заверенные копии регистрационных документов агентства, отказало ему в заключении договора на распространение указанной информации на том основании, что агентство «Велес» занимается лишь экспертизой проектов законов. Ссылаясь на письмо ЦБ РФ от 4 августа 1995 года №183 и на то, что в уставе агентства «Велес» прямо сказано о специализации его работников в области распространения любой социально-правовой информации, агентство обжаловало решение департамента в Правительство РФ.

Как разрешить этот информационно-правовой спор?

2. Фирма «Крокус» оказывала различного рода правовые услуги гражданам с использованием правовых информационно-поисковых систем «Право» и «Юрисконсульт», являвшихся её собственностью. Через год эта фирма открыла свое дочернее предприятие «Миф» и передала ему часть технических средств со всем программным обеспечением, которое ранее было установлено на них. Прошел год и предприятие «Миф» объявило себя самостоятельным и независимым от фирмы «Крокус», выкупив у неё ПК, на которых оставались правовые системы, принадлежавшие «Крокусу». Однако в своей деятельности сотрудники дочернего предприятия продолжали использовать эти информационно-поисковые системы.

Имеются ли нарушения законодательства при использовании фирмой «Крокус» и её дочерними предприятиями технических средств и программ?

3. Оператор Суманеева стала обсуждать со всеми в лаборатории перспективного программирования, откуда появилась у инженера Петровой машина и норковая шуба. Кто-то из сотрудников бросил:"А она торгует компьютерами и программами".Суманеева пошутила, сказав, что Петрова настоящая компьютерная пиратка. О разговоре тут же стало известно Петровой, и она обратилась в суд с просьбой привлечь к уголовной ответственности Суманееву за клевету и оскорбление.

Проведите анализ ситуации.

4. На закрытом химическом предприятии, расположенном в черте города и находящемся в близи от государственной границы, в результате аварии произошел выброс вредных веществ в атмосферу. Городская администрация приняла необходимые меры по эвакуации граждан из зараженных мест и

предотвращения утечки нежелательной информации об аварии. При этом она запретила руководству предприятия передавать зарубежным СМИ и специалистам информацию о масштабах, аварии и сведения, касающиеся жизни населенных пунктов, входящих в зону досягаемости распространения вредных веществ. Одновременно администрация, принимая решение о нераспространении указанной информации, ссылалась на закрытость производства химического предприятия.

Правомерны ли действия городской администрации с точки зрения норм информационного права?

5. Гражданин Петров, являвшийся сотрудником научно-исследовательского института «Прогресс», действующего в организационно-правовой форме государственного учреждения, занимался согласно должностной инструкции разработкой анализаторов радиационной обстановки. Петров считался одним из ведущих в стране специалистов по указанной тематике и являлся автором 50 изобретений, в которых воплощались новые технические решения, применяемые в анализаторах.

В октябре 2006 года Петров дал интервью корреспонденту периодического печатного издания «Метро», в котором охарактеризовал радиационную обстановку в регионе и раскрыл сущность предложенного им нового способа определения интенсивности гамма-излучения. Интервью с Петровым было опубликовано и стало достоянием общественности и руководства научно-исследовательского института «Прогресс».

Руководство института возбудило против Петрова уголовное дело по признакам преступлений, закрепленных в ст. 147 и ст. 183 УК РФ.

Адвокату Петрова в процессе ознакомления с материалами дела стало известно, что в научно-исследовательском институте существует локальный перечень сведений, составляющих коммерческую тайну, утвержденный заместителем директора НИИ, с которым сотрудник Петров был ознакомлен под роспись. В этот перечень, в частности включались и сведения о радиационной обстановке в регионе.

Адвокату кроме того стало известно, что ни в должностной инструкции Петрова ни в трудовом договоре, заключенном им с научно-исследовательским институтом не содержалось положений и условий, обязывающих Петрова создавать какие либо объекты промышленной собственности.

- по каким основаниям было возбуждено уголовное дело против Петрова?

- являются ли требования, предъявляемые к Петрову правомерными?

- имеется ли у Петрова возможность избежать уголовного наказания?

6. К руководству акционерного общества «Синтез» обратилась общественная организация «Здоровье» с просьбой представить данные о производственном травматизме на предприятии за последние три года. Руководство акционерного общества отказалось удовлетворить просьбу общественной организации, мотивируя свое отказное решение тем, что указанные данные являются секретом производства. Общественная организация повторно обратилась с аналогичной просьбой, указав в письме на имя акционерного общества на ст. 5 Федерального закона «О коммерческой тайне», согласно которой режим коммерческой тайны не может быть установлен в отношении сведений, касающихся показателей производственного травматизма. На повторное обращение общественной организации поступил повторный отказ с указанием на то, что сведения, которые не могут составлять коммерческую тайну, могут находиться в режиме секретов производства. Общественная организация была вынуждена обратиться в экспертно-правовой центр юридического факультета за получением соответствующих разъяснений.

Дайте разъяснения по существу сложившейся ситуации.

7. В прокуратуру города N обратился с заявлением лидер одной из партий, представленных в Государственной Думе. В своем заявлении он просил привлечь к уголовной ответственности одного из членов своей партии по ст. 284 УК РФ, предусматривающей уголовную ответственность за утрату документов, содержащих государственную тайну.

В ходе следствия выяснились следующие обстоятельства. Член партии Петров имел по роду своей профессиональной деятельности вторую форму допуска. Как надежному человеку ему было поручено в рамках партийных обязанностей вести списки потенциальных членов партии работающих на оборонном предприятии, а равно списки членов партии планируемых на выдвижение на высшие государственные посты. Книга с указанными сведениями, хранившаяся в штаб-квартире партии и имевшая надпись на титульном листе «секретно», регистрационный номер, дату рассекречивания, указание на партийную организацию, принявшую решение о засекречивании была утрачена. Ответственным за ее хранение был Петров. По мнению лидера партии утрата подобного рода документа могла повлечь политический кризис в стране и тем самым нанести ущерб безопасности государства.

Существует ли легальное понятие партийной тайны?

Может ли характер сведений, составляющих партийную тайну подпадать под признаки сведений, составляющих государственную тайну?

Какое решение должна принимать прокуратуру?

8. Против журналистки А, не имевшей допуска к сведениям, составляющим государственную тайну было возбуждено уголовное дело по признакам преступления, предусмотренным ст. 283 УК РФ.

Обстоятельства дела сводились к следующему.

Журналистка А предала гласности (опубликовала в газете) закрытые сведения об объемах запасов в недрах стратегического вида полезных ископаемых в России, полученные ею в ходе интервью с высокопоставленным лицом из Минэкономразвития.

Является ли журналистка А субъектом разглашения государственной тайны?

Является ли субъектом разглашения сведений, составляющих государственную тайну должностное лицо из Минэкономразвития, в функциональные обязанности которого входит работа с такими сведениями?

Может ли журналистка А быть привлечена к уголовной ответственности если в ходе интервью была предупреждена со стороны интервьюируемого, что сведения которыми он делится не подлежат распространению в силу их секретности?

Может ли журналистка А быть привлечена к уголовной ответственности как соучастник преступления?

9. Гражданин Иванов десять лет назад допускавшийся по форме один к сведениям составляющим государственную тайну и прекративший трудовые отношения с закрытым НИИ 6 лет назад обратился в паспортно-визовую службу с просьбой на получение загранпаспорта и разрешением на выезд из Российской Федерации в Великобританию. В выдаче загранпаспорта и разрешения на выезд ему было отказана. Основанием для отказа явилось заключение Межведомственной комиссии по защите государственной тайны о том, что сведения, к которым был в свое время допущен Иванов, сохраняют секретность. Иванов посчитал, что его права нарушены и обратился в коллегию адвокатов за юридической помощью.

Разрешите дело.

Заключение

Проделанная работа поможет студенту успешно пройти Интернет - тестирование и закрепить знания, полученные в процессе обучения. Таким образом, будет достигнута цель по формированию правового мировоззрения студента. Помимо этого, процесс обучения, связанный с изучением основ правоведения, поможет выработать определённую логику и культуру правового мышления, определит на будущее ценностные ориентиры и моральные установки.

Литература

1. Бачило И.Л. Информационное право: учебник – 2-е издание переработанное и дополненное. М. ИД Юрайт. 2011. 522с.
2. Рассолов И.М. Информационное право: учебник. М. ИД Юрайт. 2011. 440с.
3. Информационное право: учебник/ Л.Л. Попов, Ю.И. Мигачев, С.В. Тихомиров. М. Норма. 2010. 496с.
4. Городов О.А. Информационное право. М. 2007.
5. Правовое обеспечение информационной безопасности: Учебное пособие / под. ред. С.Я. Казанцева. М. 2005.

Методическое указание предназначено для помощи студентам в подготовке к тестированию, а так же для практических занятий по основам информационного права РФ (для всех специальностей и направлений)

Составитель: Вахтель Р.Р.

Издательство Казанского государственного архитектурно-строительного университета

Подписано в печать 30.10.12		Формат 60x84/16
Заказ № 435	Печать ризографическая	Усл. печ.л 1,31
Тираж 60 экз.	Бумага офсетная № 1	Уч.-изд.л 1,31

Отпечатано в полиграфическом секторе
Издательства КГАСУ.

420043, Казань, Зеленая, 1.