**Карта тестовых заданий**

**Компетенция** ОПК-9.2: Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей

**Индикатор**

ОПК-9.2.1: Реализует комплекс организационных мероприятий по обеспечению информационной безопасности телекоммуникационных систем и сетей

**Дисциплина** Организационное и правовое обеспечение информационной безопасности

**Описание теста:**

1. Тест состоит из 120 заданий, которые проверяют уровень освоения компетенций обучающегося. При тестировании каждому обучающемуся предлагается 30 тестовых заданий по 15 открытого и закрытого типов разных уровней сложности.
2. За правильный ответ тестового задания обучающийся получает 1 условный балл, за неправильный ответ – 0 баллов. По окончании тестирования, система автоматически определяет «заработанный итоговый балл» по тесту, согласно критериям оценки
3. Максимальная общая сумма баллов за все правильные ответы составляет – 100 баллов.
4. Тест успешно пройден, если обучающийся правильно ответил на 70% тестовых заданий (61 балл).
5. На прохождение тестирования, включая организационный момент, обучающимся отводится не более 45 минут. На каждое тестовое задание в среднем по 1,5 минуты.
6. Обучающемуся предоставляется одна попытка для прохождения компьютерного тестирования.

**Кодификатором** теста по дисциплине является раздел рабочей программы «4. Структура и содержание дисциплины (модуля)»

**Комплект тестовых заданий**

**Задания закрытого типа**

**Задания альтернативного выбора**

*Выберите* ***один*** *или* ***несколько*** *правильных ответов*

**Простые (1 уровень)**

1. Основой системы информационной безопасности объекта являются эти методы защиты

**А) Организационные, правовые, технические**

Б) Организационные, правовые, эксплуатационные

В) Организационные, методические, технические

Г) Интеллектуальные, методические, технические

1. Организационные методы защиты информации включают это…

**А) Введение режима защиты информации, подготовка и переподготовка кадров**

**В) Системы лицензирования и сертификации в области защиты информации, создание служб безопасности**

Б) Ведомственные, внутриорганизационные, государственные, международные, местные правовые акты

В) Программные, аппаратные, криптографические средства

1. Правовые методы защиты информации включают это…

А) Введение режима защиты информации, подготовка и переподготовка кадров, системы лицензирования и сертификации в области защиты информации, создание служб безопасности

**Б) Ведомственные, внутриорганизационные, государственные, международные, местные правовые акты**

В) Программные, аппаратные, криптографические средства

1. Технические методы защиты информации включают это ...

А) Введение режима защиты информации, подготовка и переподготовка кадров, системы лицензирования и сертификации в области защиты информации, создание служб безопасности

Б) Ведомственные, внутриорганизационные, государственные, международные, местные правовые акты

**В) Программные, аппаратные, криптографические средства**

1. Средства и методы защиты информации применимы к этим объектам ...

А) Комплексным

**Б) Материальным**

В) Нематериальным

Г) Простым

1. Информационное законодательство это ...

**А) Совокупность законов, нормативных актов и других форм правового регулирования в сфере обращения и производства информации и применения информационных технологий**

Б) Совокупность правовых актов, которые определяют правовое положение участников гражданского оборота, основания возникновения и порядок осуществления права собственности и других имущественных прав, прав на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации

В) Совокупность нормативных правовых актов, принимаемых уполномоченными органами государственной власти, содержащих нормы, регулирующие отношения, связанные с установлением оснований привлечения к уголовной ответственности и освобождения от неё

1. Информация это ...

А) Обобщающее понятие, описывающее различные виды объектов: простых (звук, изображение, текст, число) и комплексных структурированных (элемент, база данных, таблица, гипертекст, гипермедиа)

Б) Организационно упорядоченная совокупность массивов документов и информационных технологий, реализующая процессы сбора, хранения, обработки, поиска, распространения, передачи и предоставления информации

**В) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления**

**Г) Совокупность всей получаемой и накапливаемой информации в процессе развития науки, культуры, образования, практической деятельности людей и функционирования специальных**

1. Государственные информационные ресурсы принадлежат этим субъектам права ...

**А) Органам государственной власти и управления**

Б) Физическим лица

В) Юридическим лицам

1. Негосударственные информационные ресурсы принадлежат этим субъектам права ...

А) Органам государственной власти

Б) Органам государственного управления

**В) Физическим и юридическим лицам**

1. Персональные данные это информация, относящая к этим субъектам права...

А) Органам государственной власти

Б) Органам государственного управления

**В) Физическим лицам**

Г) Юридическим лицам

**Средне-сложные (2 уровень)**

1. Этапы защиты информации в компьютерной сети включают это ...

**А) Анализ риска, поддержание политики безопасности, реализация политики безопасности**

Б) Проектирование и планирование системы защиты информации

В) Создание политики безопасности, формирование службы защиты информации

1. Государственная тайна это ...

**А) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ**

Б) Материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов

В) Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях

1. Носители сведений, составляющих государственную тайну это ...

А) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ

В) Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях

**Б) Материальные объекты, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов**

**Б) Физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов**

1. Система защиты государственной тайны это ...

А) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ

Б) Материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов

**В) Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях**

1. Субъекты правоотношений относительно государственной тайны это ...

**А) Граждане и должностные лица, которые взяли на себя обязательство либо обязаны по своему статусу выполнять требования законодательства о государственной тайне;**

**Б) Органы государственной власти и управления; юридические лица, независимо от их организационно-правовых форм деятельности и видов собственности**

В) Информация в военной области; информация в области экономики, науки и техники; информация о внешнеполитической и внешнеэкономической деятельности

Г) Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности

1. К сведениям, составляющим государственную тайну, относят это ...

**А) Информация в военной области; информация в области экономики, науки и техники; информация о внешнеполитической и внешнеэкономической деятельности; сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности**

Б) Организованная совокупность знаний, представленная в форме, которая допускает автоматическое или автоматизированное использование этих знаний на основе реализации возможностей средств информационных технологий в области государственного и военного управления

В) Поименованная, целостная совокупность данных, которая отображает состояние объектов и их отношений в области государственного и военного управления

Г) Совокупность всех массивов информации длительного хранения, как правило, а также программно-технических средств, обеспечивающих ее накопление, обновление, корректировку и использование в области государственного и военного управления

1. В сферах экономики, науки и техники к государственной тайне относятся эту информацию ...

А) Информация в военной области; информация о внешнеполитической и внешнеэкономической деятельности

Б) Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности

**Б) Сведения о государственных программах и мероприятиях в области защиты государственной тайны; сведения о методах и средствах защиты секретной информации**

**Г) Сведения о научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение**

1. На носители сведений, составляющих государственную тайну, наносится реквизит, включающий это ...

**А) Сведения о дате или условии рассекречивания сведений; сведения о регистрационном номере; сведения о степени секретности сведений со ссылкой на соответствующий пункт перечня сведений, подлежащих засекречиванию; сведения об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя**

Б) Сведения о порядке или условии засекречивания сведений; сведения о реестровом номере; сведения о степени охраняемости сведений со ссылкой на соответствующий пункт перечня сведений, подлежащих рассекречиванию; сведения об органе государственной власти, о предприятии, об учреждении, организации, осуществивших рассекречивание носителя

1. Основанием для рассекречивания сведений, составляющих государственную тайну в РФ является это ...

**А) Взятие на себя РФ международных обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну**

**Б) Изменение обстоятельств, вследствие чего дальнейшая защита сведений является нецелесообразной**

В) Отказ РФ от международных обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну

Г) Применение обстоятельств, вследствие чего дальнейшая защита сведений является целесообразной

1. Срок засекречивания сведений, составляющих государственную тайну, не должен превышать этого времени, … лет

А) 10 лет

Б) 20 лет

В) 30 лет

Г) 40 лет

**Д) 50 лет**

1. Органы защиты государственной тайны в РФ это ...

**А) Межведомственная комиссия по защите государственной тайны РФ, МО РФ, СВР РФ, ФСБ РФ, ФСТЭК РФ**

Б) Межрегиональная комиссия по защите государственной тайны РФ, МВД РФ, Минпромторг РФ, Центробанк РФ

1. Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются эти льготы ...

А) Использование ежегодного отпуска в удобное для них время и предоставление отпуска без сохранения заработной платы сроком до 35 календарных дней в году

Б) Компенсация расходов на оплату жилых помещений в размере 50 процентов платы за наем и (или) платы за содержание жилого помещения, включающей в себя плату за услуги, работы по управлению многоквартирным домом, за содержание и текущий ремонт общего имущества в многоквартирном доме

**В) Преимущественное право при прочих равных условиях на оставление на работе при проведении организационных или штатных мероприятий**

**Г) Процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ**

1. Размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке), установленный за работу со сведениями, имеющими степень секретности «особой важности» составляет это ... в %

А) 10-15%

Б) 30-50%

**В) 50-75%**

Г) 5-10%

1. Размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке), установленный за работу со сведениями, имеющими степень секретности «совершенно секретно» составляет это ... в %

А) 10-15%

**Б) 30-50%**

В) 50-75%

Г) 5-10%

1. Размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке), установленный за работу со сведениями, имеющими степень секретности «секретно» при оформлении допуска с проведением проверочных мероприятий составляет это ... в %

**А) 10-15%**

Б) 30-50%

В) 50-75%

Г) 5-10%

1. Размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке), установленный за работу со сведениями, имеющими степень секретности «секретно» при оформлении допуска без проведения проверочных мероприятий составляет э это ... в %

А) 10-15%

Б) 30-50%

В) 50-75%

**Г) 5-10%**

1. Должностное лицо или гражданин, допущенные, или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в этих правах ...

**А) Праве выезда за границу на срок, оговоренный в трудовом договоре при оформлении допуска к государственной тайне**

**Б) Праве на неприкосновенность частной жизни при проведении проверочных мероприятий**

**В) Праве на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения**

Г) Праве невыезда за границу на срок, оговоренный в трудовом договоре при оформлении допуска к государственной тайне

Д) Праве на неприкосновенность духовной жизни при проведении проверочных мероприятий;

Е) Праве на нераспространение сведений, составляющих государственную тайну, и на неиспользование открытий и изобретений, содержащих такие сведения

1. Лицензия на проведение работ с использованием сведений, составляющих государственную тайну (ГТ), выдается предприятию при выполнении этого условия

**А) Выполнение требований, утверждаемых Правительством РФ, по обеспечению защиты ГТ**

**Б) Наличие в структуре предприятия подразделений по защите ГТ и специально подготовленных сотрудников для работы по защите информации**

**В) Наличие у предприятия сертифицированных средств защиты информации**

Г) Выполнение требований, утверждаемых Государственной Думой РФ, по обеспечению защиты ГТ

Д) Наличие в структуре предприятия подразделений по защите информации ограниченного доступа и специально подготовленных сотрудников для работы в системе электронного документооборота

Е) Наличие у предприятия аккредитованных средств защиты информации

1. Сведения конфиденциального характера включают это ...

**А) Коммерческая тайна; персональные данные; профессиональная тайна**

**Б) Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации о них**

**В) Служебная тайна; тайна следствия и судопроизводства**

Г) Корпоративная тайна; контактные данные; тайна оригинала;

Д) Сведения о сущности изобретения, полезной модели или промышленного образца после официальной публикации о них

Е) Рабочая тайна; надзорная тайна

1. Врачебная тайна это ...

**А) Информация, содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья**

Б) Сведения о страхователе, застрахованном лице и выгодоприобретателе

В) Сведения об усыновлении ребенка усыновителем

Г) Сведения, доверенные нотариусу в связи с совершением нотариальных действий

Д) Сведения, доверенные священнослужителю гражданином на исповеди

Е) Сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи

Ж) Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

1. Тайна связи это ...

А) Информация, содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья

Б) Сведения о страхователе, застрахованном лице и выгодоприобретателе

В) Сведения об усыновлении ребенка усыновителем

Г) Сведения, доверенные нотариусу в связи с совершением нотариальных действий

Д) Сведения, доверенные священнослужителю гражданином на исповеди

Е) Сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи

(**Ж)Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений**)

1. Нотариальная тайна это ...

А) Информация, содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья

Б) Сведения о страхователе, застрахованном лице и выгодоприобретателе

В) Сведения об усыновлении ребенка усыновителем

**Г) Сведения, доверенные нотариусу в связи с совершением нотариальных действий**

Д) Сведения, доверенные священнослужителю гражданином на исповеди

Е) Сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи

Ж) Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

1. Адвокатская тайна включает это ...

А) Информация, содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья

Б) Сведения о страхователе, застрахованном лице и выгодоприобретателе

В) Сведения об усыновлении ребенка усыновителем

Г) Сведения, доверенные нотариусу в связи с совершением нотариальных действий

Д) Сведения, доверенные священнослужителю гражданином на исповеди

**Е) Сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи**

Ж) Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

1. Тайна усыновления включает это ...

А) Информация, содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья

Б) Сведения о страхователе, застрахованном лице и выгодоприобретателе

**В) Сведения об усыновлении ребенка усыновителем**

Г) Сведения, доверенные нотариусу в связи с совершением нотариальных действий

Д) Сведения, доверенные священнослужителю гражданином на исповеди

Е) Сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи

Ж) Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

1. Тайна страхования включает это ...

А) Информация, содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья

**Б) Сведения о страхователе, застрахованном лице и выгодоприобретателе**

В) Сведения об усыновлении ребенка усыновителем

Г) Сведения, доверенные нотариусу в связи с совершением нотариальных действий

Д) Сведения, доверенные священнослужителю гражданином на исповеди

Е) Сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи

Ж) Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

1. Тайна исповеди включает это ...

А) Информация, содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья

Б) Сведения о страхователе, застрахованном лице и выгодоприобретателе

В) Сведения об усыновлении ребенка усыновителем

Г) Сведения, доверенные нотариусу в связи с совершением нотариальных действий

**Д) Сведения, доверенные священнослужителю гражданином на исповеди**

Е) Сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи

Ж) Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

**Сложные (3 уровень)**

1. Коммерческая тайна это ...

А) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ

Б) Информация, содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья

**В) Конфиденциальная информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду**

Г) Сведения о страхователе, застрахованном лице и выгодоприобретателе

Д) Сведения об усыновлении ребенка усыновителем

Е) Сведения, доверенные нотариусу в связи с совершением нотариальных действий

Ж) Сведения, доверенные священнослужителю гражданином на исповеди

З) Сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи

И) Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

1. Злоумышленник это ...

А) Лицо или группа лиц, занимающихся текущим управлением базой данных и отвечающих за технологию ее работы

Б) Лицо или группа лиц, занимающихся текущим управлением сети и перспективой ее развития

В) Объект, который незаконным путем пытается добыть, изменить или уничтожить информацию законных пользователей

**Г) Субъект, который незаконным путем пытается добыть, изменить или уничтожить информацию законных пользователей**

1. Защита информации является этой задачей ...

А) Легко-формализуемой задачей

Б) Не-формализуемой задачей

**В) Слабо-формализуемой задачей**

Г) Условно-формализуемой задачей

1. В основе решения задачи защиты информации лежит этот подход ...

А) Буферный подход

Б) Корреляционный подход

**В) Системный подход**

Г) Условный подход

1. Угроза безопасности информации – совокупность условий и факторов, создающих это ...

**А) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации**

Б) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность системе управления любым объектом, реализующей возможности информационных и коммуникационных технологий, в которой человек принимает непосредственное участие

В) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность комплексу технических, программных и методических средств, обслуживающих рабочее место пользователя, обеспечивающий осуществление информационной деятельности, информационного взаимодействия и доступ к информационным ресурсам

Г) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность лицу или группе лиц, занимающихся текущим управлением базой данных и отвечающих за технологию ее работы

1. Атака на информационный ресурс это ...

**А) Попытка реализации угрозы**

Б) Попытка угрозы реализации

В) Реализация попытки угрозы

Г) Угроза реализации попытки

1. Источник угрозы безопасности информации – субъект (физическое лицо, материальный объект или физическое явление), являющийся, управляющий, занимающийся этим ...

**А) Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации**

Б) Субъект (физическое лицо, материальный объект или физическое явление), управляющий информационной системой, взаимодействующий с пользователями, обеспечивающий надежность ее функционирования

В) Субъект (физическое лицо, материальный объект или физическое явление), занимающийся обеспечением надежности функционирования, поддержанием целостности, обеспечением санкционированного доступа, реструктуризацией, актуализацией данных и пр.

Г) Субъект (физическое лицо, материальный объект или физическое явление), занимающийся обеспечением надежности функционирования сети, определение и выдачей адресов и паролей доступа, обеспечением взаимодействия с другими сетями, взаимодействием с администраторами базы данных и пр.

1. Цель защиты информации — это обеспечение …

**А) Обеспечение информационной безопасности**

Б) Обеспечение технической безопасности

В) Обеспечение технологической безопасности

Г) Обеспечение техносферной безопасности

1. Конфиденциальность — это состояние информации, при котором доступ к ней осуществляют…

А) Состояние информации, при котором доступ к ней осуществляют все субъекты

**Б) Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право**

В) Состояние информации, при котором доступ к ней осуществляют только субъекты – органы государственной власти и управления

Г) Состояние информации, при котором доступ к ней осуществляют только хозяйствующие субъекты

1. Целостность информации — это состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется (осуществляют) ...

А) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно всеми субъектами

**Б) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право**

В) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляют только субъекты – органы государственной власти и управления

Г) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляют только хозяйствующие субъекты

1. Доступность информации — это состояние информации, при котором субъекты, имеющие права доступа ...

А) Состояние информации, при котором субъекты, имеющие права доступа, не могут реализовать их беспрепятственно

Б) Состояние информации, при котором субъекты, имеющие права доступа, не могут реализовать их бескорыстно

**В) Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно**

Г) Состояние информации, при котором субъекты, не имеющие права доступа, могут реализовать их беспрепятственно

1. Правовая защита информации это ...

А) Защита информации организационными методами, включающая в себя разработку организационных документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

**Б) Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением**

В) Защита информации техническими методами, включающая в себя разработку технических документов (регламентов), регулирующих отношения субъектов по защите информации, применение этих документов (регламентов), а также надзор и контроль за их исполнением

Г) Защита информации технологическими методами, включающая в себя разработку технологических документов (регламентов), регулирующих отношения субъектов по защите информации, применение этих документов (регламентов), а также надзор и контроль за их исполнением

1. Организационные меры защиты информации — это меры ...

**А) Меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой**

Б) Меры технического характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой

В) Меры технологического характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой

Г) Меры физического характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой

1. Физическая защита информации — это совокупность ...

А) Совокупность организационных документов, препятствующих физическому проникновению потенциального злоумышленника в контролируемую зону

Б) Совокупность организационных документов, препятствующих физическому проникновению потенциального злоумышленника в контролируемую зону

В) Совокупность правовых документов, препятствующих физическому проникновению потенциального злоумышленника в контролируемую зону

**Г) Совокупность средств, препятствующих физическому проникновению потенциального злоумышленника в контролируемую зону**

1. Концептуальные документы в области защиты информации это ...

А) Гражданский кодекс РФ

**Б) Доктрина информационной безопасности РФ**

В) Трудовой кодекс РФ

Г) Уголовный кодекс РФ

**Задания на установление соответствия**

*Установите соответствие между левым и правым столбцами*.

**Простые (1 уровень)**

1. Установите соответствие определений

|  |  |
| --- | --- |
| 1) Совокупность законов, нормативных актов и других форм правового регулирования в сфере обращения и производства информации и применения информационных технологий2) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления3) Сведения, относящаяся к определенному физическому лицу | 1. Информационное законодательство
2. Информация
3. Персональные данные
4. Информационные отношения
 |

1. Установите соответствие определений

|  |  |
| --- | --- |
| 1) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ2) Материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов3) Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях | 1. Государственная тайна
2. Носители сведений, составляющих государственную тайну
3. Система защиты государственной тайны
4. Защита государственной тайны
 |

1. Установите соответствие надбавки

|  |  |
| --- | --- |
| 1) Размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке), установленный за работу со сведениями, имеющими степень секретности «особой важности»2) Размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке), установленный за работу со сведениями, имеющими степень секретности «совершенно секретно»3) Размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке), установленный за работу со сведениями, имеющими степень секретности «секретно» при оформлении допуска с проведением проверочных мероприятий4) Размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке), установленный за работу со сведениями, имеющими степень секретности «секретно» при оформлении допуска без проведения проверочных мероприятий | А) 50-75%Б) 30- 50%В) 10-15%Г) 5-10%Д) 1-5% |

1. Установите соответствие определений

|  |  |
| --- | --- |
| 1) Исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполненных работ или услуг (фирменное наименование, товарный знак и пр.)2) Базы данных, изобретения, исполнения; коммерческие обозначения, наименования мест происхождения товаров, полезные модели; программы для электронных вычислительных машин (ЭВМ), произведения науки, литературы и искусства, промышленные образцы; секреты производства (ноу-хау), селекционные достижения, сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания); товарные знаки и знаки обслуживания, топологии интегральных микросхем, фирменные наименования, фонограммы3) Физическое лицо, творческим трудом которого создано произведение4) Зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы и связей между ними | 1. Интеллектуальная собственность
2. Результаты интеллектуальной деятельности
3. Автор
4. Топология
5. Охрана интеллектуальной деятельности
 |

1. Установите соответствие форм

|  |  |
| --- | --- |
| 1) Форма правовой защиты в отношении литературных, художественных и научных произведений2) Форма правовой защиты в отношении изобретений во всех областях человеческой деятельности3) Форма правовой защиты любых полезных сведения (производственных, технических, экономических, организационных и пр.) | 1. Авторское право
2. Патентное право
3. Секреты производства (ноу-хау)
4. Коммерческое право
 |

**Средне-сложные (2 уровень)**

1. Установите соответствие определений

|  |  |
| --- | --- |
| 1) Введение режима защиты информации; подготовка и переподготовка кадров; системы лицензирования и сертификации в области защиты информации; создание служб безопасности2) Ведомственные, внутриорганизационные, государственные, международные, местные правовые акты3) Программные, аппаратные, криптографические средства; физические ограждения и препятствия | 1. Организационные методы защиты информации
2. Правовые методы защиты информации
3. Технические методы защиты
4. Технологические методы защиты
 |

1. Установите соответствие кодификаторов Интерпола

|  |  |
| --- | --- |
| 1) Методы несанкционированного доступа к информации2) Изменение компьютерных данных3) Компьютерное мошенничество4) Незаконное копирование QR5) Компьютерный саботаж QS6) Прочие компьютерные преступления | 1. QA
2. QD
3. QF
4. QR
5. QS
6. QZ
7. QN
 |

1. Установите соответствие методов

|  |  |
| --- | --- |
| 1) Установка микрофона в компьютере с целью перехвата разговоров обслуживающего персонала2) Сбор информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе3) Поиск данных, оставленных пользователем после работы на компьютере4) Несанкционированное проникновение, как в пространственные, так и в электронные закрытые зоны5) Возможность подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе | 1. Метод «Жучок»
2. Метод «Откачивание данных»
3. Метод «Уборка мусора»
4. Метод «Следование за дураком»
5. Метод «За хвост»
6. Метод «Поиск вечности»
 |

1. Установите соответствие методов

|  |  |
| --- | --- |
| 1) Несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем2) Использование ошибок или неудач в логике построения программы, когда бреши могут применяться неоднократно3) В найденной «бреши» программа «разрывается» и туда вставляется определенное число команд4) Злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя5) Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать информацию | 1. Метод «Неспешного выбора»
2. Метод «Поиск бреши»
3. Метод «Люк»
4. Метод «Маскарад»
5. Метод «Мистификация»
6. Метод «Поиск бесконечности»
 |

1. Установите соответствие принципов в области обеспечения информационной безопасности

|  |  |
| --- | --- |
| 1) Минимизация привилегий; разделение обязанностей2) Распределение роли и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс3) Введение пользователям только тех прав доступа, которые необходимы им для выполнения служебных обязанностей | 1. Управления персоналом
2. Разделения обязанностей
3. Минимизации привилегий
4. Управления проектами
 |

1. Установите соответствие процессов

|  |  |
| --- | --- |
| 1) Процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдает2) Процесс, в ходе которого выясняются права доступа, привилегии, свойства и характеристики пользователя на основании его имени, логина или какой-либо другой информации о нем3) Процесс входа в систему, когда пользователь вводит два кода: свое условное имя (идентификация) и уникальный, известный только ему одному код-пароль для аутентификации  | 1. Аутентификация
2. Идентификация
3. Парольный метод
4. Интенсификация
 |

**Сложные (3 уровень)**

1. Укажите последовательность этапов проектирования системы физической защиты объекта информатизации

1)Концептуальное проектирование А) 1

2)Рабочее проектирование Б) 2

3)Системное проектирование В) 3

 Г) 4

1. Укажите принципы организационной защиты информации

|  |  |
| --- | --- |
| 1) Эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации2) Существенное влияние на эффективность функционирования и гибкость системы защиты информации и отражение нацеленности руководства и персонала предприятия на решение задач защиты информации3) Эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения | 1. Комплексного подхода
2. Оперативности принятия решений
3. Персональной ответственности
4. Интеллектуального подхода
 |

1. Укажите виды защиты информации

|  |  |
| --- | --- |
| 1) Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением2) Защита информации, заключающаяся в обеспечении не криптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств3) Защита информации с помощью ее криптографического преобразования4) Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты | 1. Правовая
2. Техническая
3. Криптографическая
4. Физическая
5. Технологическая
 |

1. Укажите виды тайн

|  |  |
| --- | --- |
| 1) Сведения научно-технического, экономического, политического и военного характера, разглашение или утрата которых представляет угрозу для безопасности государства2) Сведения, охраняемые государством, чисто военного характера3) Сведения, утрата и разглашение которых приносит ущерб интересам государства | А) ГосударственнаяБ) ВоеннаяВ) СлужебнаяГ) Корпоративная |

1. Укажите соответствие форм допуска, дающие право на ознакомление с секретными сведениями

**1) Особой важности, совершенно секретно, секретно А) Первая**

**2) Совершенно секретно, секретно Б) Вторая**

**3) Секретно В) Третья**

 **Г) Четвертая**

**Задания открытого типа**

**Задания на дополнение**

*Напишите пропущенное слово.*

**Простые (1 уровень)**

1. Информация, содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья – это ... тайна (**Врачебная**)
2. Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений – это тайна ...(**Связи**)
3. Сведения, доверенные нотариусу в связи с совершением нотариальных действий – это ... тайна (**Нотариальная**)
4. Сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи – это ... тайна (**Адвокатская**)
5. Сведения об усыновлении ребенка усыновителем – это тайна ... (**Усыновления**)
6. Сведения о страхователе, застрахованном лице и выгодоприобретателе – это тайна ... (**Страхования**)
7. Сведения, доверенные священнослужителю гражданином на исповеди – это тайна ... (**Исповеди**)
8. Уголовная ответственность наступает в случае разглашения тайны ... (**Связи, Усыновления**)
9. Государственные информационные ресурсы принадлежат – органам... (**Государственной власти и управления**)
10. Негосударственные информационные ресурсы принадлежат – ... лицам (**Физическим, Юридическим**)

**Средне-сложные (2 уровень)**

1. Срок засекречивания сведений, составляющих Государственную тайну, не должен превышать – ... лет **(50)**
2. Средства и методы защиты информации применимы – к ... объектам (**Материальным**)
3. Совокупность законов, нормативных актов и других форм правового регулирования в сфере обращения и производства информации и применения информационных технологий – это ... законодательство (**Информационное**)
4. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления – это ... (**Информация**)
5. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ – это ... тайна (**Государственная**)
6. Материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну (ГТ), находят свое отображение в виде символов, образов, сигналов, технических решений и процессов – это ... (**Носители сведений ГТ**)
7. Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну (ГТ), и их носителей, а также мероприятий, проводимых в этих целях – это ... (**Система защиты ГТ**)
8. Система защиты государственных секретов в РФ основывается на Законе – ... (**О Государственной тайне**)
9. Нарушения законодательства в области налоговой тайны (НТ) – это ... (**Разглашение НТ, Утрата документов, содержащих НТ**)
10. Незаконное использование секретной информации лицом или предприятием, не уполномоченным на то ее владельцем; а также, незаконный сбор сведений, составляющих коммерческую тайну – это ... шпионаж (**Промышленный**)
11. Сбор и обработка информации законными способами – это ... разведка (**Конкурентная**)
12. Конфиденциальная информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду – это ... тайна (**Коммерческая**)
13. Гриф конфиденциальности для обозначения степени важности коммерческой информации предприятия - это ... (**Для внутреннего использования (ДВИ), Коммерческая тайна – конфиденциально (КТ-К), Коммерческая тайна – строго конфиденциально (КТ-СК), Коммерческая тайна (КТ)**)
14. Субъект, который незаконным путем пытается добыть, изменить или уничтожить информацию законных пользователей – это субъект - ...

(**Злоумышленник**)

1. Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения целостности, конфиденциальности и доступности информации - это угроза ... информации (**Безопасности**)
2. Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации - это ... безопасности информации (**Источник**)
3. Обеспечение информационной безопасности - это цель ... (**Защиты информации**)
4. Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право - это ... информации (**Конфиденциальность**)
5. Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право - это ... информации (**Целостность**)
6. Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно - это ... информации (**Доступность**)
7. Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением - это ... защита информации (**Правовая**)
8. Совокупность средств, препятствующих физическому проникновению потенциального злоумышленника в контролируемую зону - это средства ... защиты информации (**Физической**)
9. Концептуальный документ в области информационной безопасности в РФ - это ... информационной безопасности (**Доктрина**)
10. Принцип управления персоналом в области обеспечения информационной безопасности - это принцип ... (**Минимизации привилегий, Разделения обязанностей**)
11. Распределение роли и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс, предписывает принцип ... (**Разделения обязанностей**)
12. Выделение пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей, предписывает принцип ... (**Минимизации привилегий**)
13. Процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдает – это процесс ... (**Аутентификации**)
14. Процесс, в ходе которого выясняются права доступа, привилегии, свойства и характеристики пользователя на основании его имени, логина или какой-либо другой информации о нем – это процесс ... (**Идентификации**)

**Сложные (3 уровень)**

1. Процесс входа в систему в ходе которого пользователь вводит два кода: свое условное имя (идентификатор) и уникальный, известный только ему одному код-пароль для аутентификации – это ... метод идентификации и аутентификации (**Парольный**)
2. Анализ ресурсов информационной системы (ИС), проводимый оперативно, или периодически – это ... ИС (**Аудит**)
3. Сбор и накопление информации о событиях, происходящих в информационной системе (ИС) - это ... ИС (**Протоколирование**)
4. В криптографии используется ... шифрование (**Асимметричное, Симметричное**)
5. Установленный нормами права единый порядок в РФ обращения со сведениями, составляющими государственную и служебную тайны - это ... (**Режим секретности**)
6. Текстовые и графические материалы, выполненные любым способом, кино-, фото- и видео-позитивы и негативы, магнитные ленты звуко- и видео-записи, перфокарты, перфоленты и другие материалы, которые содержат секретную информацию – это ... (**Секретный документ**)
7. Засекреченные образцы и комплексы вооружения и военной техники, оборудование, входящее в их состав, комплектующие узлы и элементы, материалы и вещества, которые используются при создании и вооружении военной техники – это … (**Секретное изделие**)
8. Научно-исследовательские и опытно-конструкторские, проектные, диссертационные, дипломные и другие работы, в процессе выполнения которых образуются секретные сведения – это ... (**Секретная работа**)
9. Граждане РФ, которые по своим деловым, политическим и моральным качествам способны обеспечить сохранность доверенных им тайн, могут быть допущены к ... работам и документам (**Секретным**)
10. Официальное разрешение руководителя предприятия на право выполнения закрытых работ, на право ознакомления с секретными работами и документами - это ... к государственной тайне (**Допуск**)

**Задания свободного изложения**

*Напишите развернутый ответ в свободной форме, изложив основные положения, факты, применив важнейшие понятия и сделав обобщение по теме задания*

Простые (1 уровень)

1. Правовая защита конфиденциальной информации

Средне-сложные (2 уровень)

1. Допуск к секретным работам и документам
2. Засекречивание сведений в связи с наличием в них государственных и служебных тайн
3. Лицензирование и сертификация в области защиты конфиденциальной информации

Сложные (3 уровень)

1. Классификация компьютерных преступлений по кодификатору Интерпола – несанкционированный доступ и перехват информации

**Карта учета тестовых заданий**

|  |  |
| --- | --- |
| Компетенция | ОПК-9.2: Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей |
| Индикатор | ОПК-9.2.1: Реализует комплекс организационных мероприятий по обеспечению информационной безопасности телекоммуникационных систем и сетей |
| Дисциплина | Организационное и правовое обеспечение информационной безопасности |
| Уровень освоения | Тестовые задания | Итого |
| Закрытого типа | Открытого типа |  |
| Альтернативный выбор | Установление соответствия/ последовательности | На дополнение | Свободного изложения |
| 1.1.1 (20%) | 10 | 5 | 10 | 1 | 25 |
| 1.1.2 (70%) | 26 | 5 | 27 | 3 | 58 |
| 1.1.3 (10%) | 15 | 5 | 10 | 1 | 30 |
| Итого: | 51 шт. | 15 шт. | 47 шт. | 5 шт. | 113 шт. |

**Критерии оценивания**

**Критерии оценивания тестовых заданий**

Критерии оценивания: правильное выполнение одного тестового задания оценивается 1 баллом, неправильное – 0 баллов.

Максимальная общая сумма баллов за все правильные ответы составляет наивысший балл – 100 баллов.

**Шкала оценивания результатов компьютерного тестирования обучающихся** (рекомендуемая)

|  |  |  |
| --- | --- | --- |
| Оценка  | Процент верных ответов | Баллы |
| «удовлетворительно» | 70-79% | 61-75 баллов |
| «хорошо» | 80-90% | 76-90 баллов |
| «отлично» | 91-100% | 91-100 баллов |

**Ключи ответов**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ тестовых заданий** | **Номер и вариант правильного ответа** |  |  | № | **Ключ ответа** |
|  | А) Организационные, правовые, технические |  |  |  | 1:А,2:Б,3:В,4:Г,5:Д |
|  | А) Введение режима защиты информации, подготовка и переподготовка кадровВ) Системы лицензирования и сертификации в области защиты информации, создание служб безопасности |  |  |  | 1:А,2:Б,3:В,4:Г,5:Д |
|  | Б) Ведомственные, внутриорганизационные, государственные, международные, местные правовые акты |  |  |  | 1:А,2:Б,3:В |
|  | В) Программные, аппаратные, криптографические средства |  |  |  |  |
|  | Б) Материальным |  |  |  | 1:А,2:Б,3:В |
|  | А) Совокупность законов, нормативных актов и других форм правового регулирования в сфере обращения и производства информации и применения информационных технологий |  |  |  | 1:А,2:Б,3:В |
|  | В) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представленияГ) Совокупность всей получаемой и накапливаемой информации в процессе развития науки, культуры, образования, практической деятельности людей и функционирования специальных |  |  |  | 1:А,2:Б,3:В |
|  | А) Органам государственной власти и управления |  |  |  | 1:А,2:Б,3:В,4:Г |
|  | В) Физическим и юридическим лицам |  |  |  | 1:А,2:Б,3:В |
|  | В) Физическим лицам |  |  |  | 1:А,2:Б,3:В |
|  | А) Анализ риска, поддержание политики безопасности, реализация политики безопасности |  |  |  | Врачебная |
|  | А) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ |  |  |  | Связи |
|  | Б) Материальные объекты, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессовБ) Физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов |  |  |  | Нотариальная |
|  | В) Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях |  |  |  | Адвокатская |
|  | А) Граждане и должностные лица, которые взяли на себя обязательство либо обязаны по своему статусу выполнять требования законодательства о государственной тайне; Б) Органы государственной власти и управления; юридические лица, независимо от их организационно-правовых форм деятельности и видов собственности |  |  |  | Усыновления |
|  | А) Информация в военной области; информация в области экономики, науки и техники; информация о внешнеполитической и внешнеэкономической деятельности; сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности |  |  |  | Страхования |
|  | В) Сведения о государственных программах и мероприятиях в области защиты государственной тайны; сведения о методах и средствах защиты секретной информацииГ) Сведения о научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение |  |  |  |  Исповеди |
|  | А) Сведения о дате или условии рассекречивания сведений; сведения о регистрационном номере; сведения о степени секретности сведений со ссылкой на соответствующий пункт перечня сведений, подлежащих засекречиванию; сведения об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя |  |  |  | Связи, Усыновления |
|  | А) Взятие на себя РФ международных обязательств по открытому обмену сведениями, составляющими в РФ государственную тайнуБ) Изменение обстоятельств, вследствие чего дальнейшая защита сведений является нецелесообразной |  |  |  | Государственной власти и управления |
|  | Д)50 лет |  |  |  | Физическим, Юридическим |
|  | А) Межведомственная комиссия по защите государственной тайны РФ, МО РФ, СВР РФ, ФСБ РФ, ФСТЭК РФ |  |  |  | МО РФ, СВР РФ, ФСБ РФ, ФСТЭК РФ |
|  | В) Преимущественное право при прочих равных условиях на оставление на работе при проведении организационных или штатных мероприятийГ) Процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ |  |  |  | Материальным |
|  | В)50-75% |  |  |  | Информационное |
|  | Б)30-50% |  |  |  | Информация |
|  | А)10-15% |  |  |  | Государственная |
|  | Г)5-10% |  |  |  | Носители сведений ГТ |
|  | А) Праве выезда за границу на срок, оговоренный в трудовом договоре при оформлении допуска к государственной тайнеБ) Праве на неприкосновенность частной жизни при проведении проверочных мероприятийВ) Праве на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения |  |  |  | Система защиты ГТ |
|  | А) Выполнение требований, утверждаемых Правительством РФ, по обеспечению защиты ГТБ) Наличие в структуре предприятия подразделений по защите ГТ и специально подготовленных сотрудников для работы по защите информацииВ) Наличие у предприятия сертифицированных средств защиты информации |  |  |  | О Государственной тайне |
|  | А) Коммерческая тайна; персональные данные; профессиональная тайнаБ) Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации о нихВ) Служебная тайна; тайна следствия и судопроизводства |  |  |  | Разглашение НТ, Утрата документов, содержащих НТ |
|  | А) Информация, содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья |  |  |  | Промышленный |
|  | Ж) Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений |  |  |  | Конкурентная |
|  | Г) Сведения, доверенные нотариусу в связи с совершением нотариальных действий |  |  |  | Коммерческая |
|  | Е) Сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи |  |  |  | Для внутреннего использования (ДВИ), Коммерческая тайна – конфиденциально (КТ-К), Коммерческая тайна – строго конфиденциально (КТ-СК), Коммерческая тайна (КТ) |
|  | В) Сведения об усыновлении ребенка усыновителем |  |  |  | Злоумышленник |
|  | Б) Сведения о страхователе, застрахованном лице и выгодоприобретателе |  |  |  | Безопасности |
|  | Д) Сведения, доверенные священнослужителю гражданином на исповеди |  |  |  | Источник |
|  | В) Конфиденциальная информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду |  |  |  | Защиты информации |
|  | Г) Субъект, который незаконным путем пытается добыть, изменить или уничтожить информацию законных пользователей |  |  |  | Конфиденциальность |
|  | В) Слабо-формализуемой задачей |  |  |  | Целостность |
|  | В) Системный подход |  |  |  | Доступность |
|  | А) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации |  |  |  | Правовая |
|  | А) Попытка реализации угрозы |  |  |  | Физической |
|  | А) Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации |  |  |  | Доктрина |
|  | А) Обеспечение информационной безопасности |  |  |  | Минимизации привилегий, Разделения обязанностей |
|  | Б) Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право |  |  |  | Разделения обязанностей |
|  | Б) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право |  |  |  | Минимизации привилегий |
|  | В) Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно |  |  |  | Аутентификации |
|  | Б) Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением |  |  |  | Идентификации |
|  | А) Меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой |  |  |  | Парольный |
|  | Г) Совокупность средств, препятствующих физическому проникновению потенциального злоумышленника в контролируемую зону |  |  |  | Аудит |
|  | Б) Доктрина информационной безопасности РФ |  |  |  | Протоколирование |
|  | 1:А,2:Б,3:В |  |  |  | Асимметричное, Симметричное |
|  | 1:А,2:Б,3:В |  |  |  | Режим секретности |
|  | 1:А,2:Б,3:В,4:Г |  |  |  | Секретный документ |
|  | 1:А,2:Б,3:В,4:Г |  |  |  | Секретное изделие |
|  | 1:А,2:Б |  |  |  | Секретная работа |
|  | 1:А,2:Б,3:В |  |  |  | Секретным |
|  | 1:А,2:Б,3:В,4:Г,5:Д,6:Е |  |  |  | Допуск |
| 116. | В действующем законодательстве РФ упоминается более 40 видов тайн (банковская, налоговая, коммерческая, профессиональная и т.д.), требующих введения режима конфиденциальности, и их число постоянно увеличивается. Указом Президента РФ от 06.03.97 г. № 188 был утвержден Перечень сведений «конфиденциального характера», где указаны шесть видов такой информации:* персональные данные;
* тайна следствия и судопроизводства;
* служебная тайна;
* профессиональная тайна;
* коммерческая тайна;
* сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации о них.

В соответствии с нормами международного права и Конституции РФ данный перечень должен быть в дальнейшем утвержден законом. Конфиденциальность сведений отражает гриф, устанавливаемый на материальном носителе информации. Для обозначения грифа конфиденциальности используются международные и национальные нормативные документы. Причем требования российского законодательства отличаются от утвержденных стандартов ISO 17799 «Безопасность информационных международных стандартов». Так в соответствии с ISO 17799 используются следующие обозначения:* ОТ – открытая информация;
* КИ – конфиденциальная информация;
* СКИ – строго конфиденциальная информация.

В российском законодательстве используются следующие грифы конфиденциальности:* ОТ – открытая информация;
* ДВИ – для внутреннего использования;
* КИ – конфиденциальная информация.
 |
| 117. | К секретным работам и документам могут быть допущены только граждане РФ, которые по своим деловым, политическим и моральным качествам способны обеспечить сохранность доверенных им тайн. К секретным работам и документам не допускаются лица, имеющие: психические заболевания; лица, которые понесли уголовную ответственность; лица, совершающие поступки, несовместимые с принципами нравственности и морали; лица, имеющие постоянный контакт с лицами (родственниками) за границей. На каждое лицо, допускаемое к секретным работам и документам, оформляется допуск, то есть официальное разрешение руководителя предприятия на право выполнения закрытых работ, на право ознакомления с секретными работами и документами. Существует три формы допуска к секретным работам и документам:1. Наивысшая форма допуска (имеют право на ознакомление со сведениями ОВ, СС, С).
2. Вторая форма допуска (имеют право на ознакомление со сведениями СС, С).
3. Третья форма допуска (имеют право на ознакомление со сведениями С).

При командировке сотрудников, имеющих допуск по месту основной работы, на другие предприятия им в первом отделе своего предприятия выдаются справки о допуске к секретным работам и документам, и выписываются командировочные предписания на право выполнения работ. |
| 118. | Засекречивание сведений в связи с наличием в них государственных и служебных тайн осуществляется в соответствии с перечнем главнейших сведений, составляющих государственную тайну, и ведомственными перечнями сведений, подлежащих засекречиванию. Единый порядок засекречивания сведений определен положением о порядке установления степени секретности сведений, содержащихся в работах, документах и изделиях. При засекречивании сведений руководствуются следующими принципами: * решение проблемы засекречивания в целом с позиции государственной значимости этих сведений; при этом необходимо учитывать противоречивость и единство двух тенденций: с одной стороны, стремление обеспечить надежность сохранности государственных и служебных тайн, с другой стороны, не допустить необоснованного массового засекречивания;
* объективный характер определения степени секретности сведений, который основывается на точном использовании существующих перечней охраняемых сведений;
* оптимизация объема засекречиваемых сведений;

периодический просмотр степени секретности сведений на предмет снятия или снижения грифа секретности. |
| 119 | Лицензирование деятельности в области защиты конфиденциальной информации основано на Законе РФ «О лицензировании отдельных видов деятельности» от 8 августа 2001 г. № 128-ФЗ (ред. от 11 марта 2003 г. № 32-ФЗ).Действие данного закона не распространяется на следующие виды деятельности, связанные с ЗИ:* деятельность, связанная с защитой государственной тайны;
* деятельность в области связи;
* использование результатов интеллектуальной деятельности.

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

Постановление Правительства РФ от 23.04.96 № 509 устанавливает порядок сертификации средств защиты информации в РФ и ее учреждениях за рубежом. Это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.Положение о сертификации средств защиты информации по требованиям безопасности информации ведено в действие приказом Председателя Гостехкомиссии России от 27 октября 1995 г. № 199. В соответствии с которым обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для защиты информации, составляющей государственную тайну, и другой информации с ограниченным доступом, а также средства, использующиеся в управлении экологически опасными объектами. В остальных случаях сертификация носит добровольный характер (добровольная сертификация) и осуществляется по инициативе разработчика, изготовителя или потребителя средства защиты информации.Сертификационные испытания средств защиты в рамках данной системы сертификации предусматривают комплекс мероприятий по проверке соответствия этих средств формальным базовым требованиям по обеспечению безопасности информации, изложенным в нормативных документах ФСТЭК. |
| 120. | По кодификатору Интерпола (в 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен в более чем 100 странах) все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q.Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.* 1. QA – Несанкционированный доступ и перехват.
	2. QD – Изменение компьютерных данных.
	3. QF – Компьютерное мошенничество.
	4. QR – Незаконное копирование.
	5. QS – Компьютерный саботаж.
	6. QZ – Прочие компьютерные преступления.

Несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений:1. QAH – «Компьютерный абордаж» (хакинг - hacking): неправомерный доступ в компьютер или сеть. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.
2. QAI – перехват (interception): перехват при помощи технических средств. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup).
3. Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата.
4. QAT – кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.
5. Для характеристики методов несанкционированного доступа и перехвата информации используется следующая терминология:
6. «Жучок» (bugging) – характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала.
7. «Откачивание данных» (data leakage) – отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе.
8. «Уборка мусора» (scavening) – характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.д.; электронный вариант требует исследования данных, оставленных в памяти машины.
9. Метод следования «За дураком» (piggbackiiig) – характеризует несанкционированное проникновение, как в пространственные, так и в электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним.
10. Метод «За хвост» (between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе.
11. Метод «Неспешного выбора» (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости.
12. Метод «Поиск бреши» (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно.
13. Метод «Люк» (trapdoor), являющийся развитием предыдущего. В найденной «бреши» программа «разрывается» и туда вставляется определенное число команд. По мере необходимости «люк» открывается, а встроенные команды автоматически осуществляют свою задачу.
14. Метод «Маскарад» (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя.

Метод «Мистификация» (spoofing), который используется при случайном подключении «чужой» системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например, коды пользователя. |