**Смоленское областное государственное автономное учреждение**

**«Центр информационных технологий»**

|  |
| --- |
| УТВЕРЖДАЮ |
| Директор СОГАУ «ЦИТ» |
|  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.М. Гильденков |
|  |
| «\_\_\_» \_\_\_\_\_\_\_\_\_ 2024 г. |
| м.п. |

**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА**

**повышения квалификации**

**«Защита информации с использованием криптографических средств»**

Смоленск, 2023

**Содержание**

[1. Введение. Цель реализации программы 3](#_Toc140058129)

[2. Планируемые результаты обучения 3](#_Toc140058130)

[3. Требования к квалификации лиц, поступающих на обучение 5](#_Toc140058131)

[4. Форма обучения 5](#_Toc140058132)

[5. Учебно-тематический план дополнительной профессиональной программы повышения квалификации «Защита информации с использованием криптографических средств» 5](#_Toc140058133)

[6. Календарный учебный график 7](#_Toc140058134)

[7. Программы учебных тем 7](#_Toc140058135)

[8. Условия реализации программы 16](#_Toc140058136)

[9. Форма аттестации 16](#_Toc140058137)

[10. Оценочные материалы 16](#_Toc140058138)

[11. Список литературы 25](#_Toc140058139)

# **1. Введение. Цель реализации программы**

**Целью реализации** повышения квалификации «Защита информации с использованием криптографических средств» (далее по тексту – учебная программа) является обеспечение заданного уровня знаний, умений и навыков у специалистов и пользователей в применении способов и средств обеспечения защиты информации с использованием криптографических средств в информационных системах предприятий, организаций и учреждений (далее – организации) при решении задач по организационной и технической защите обрабатываемой у них информации.

В данном документе под криптографической защитой информации (КЗИ) понимается обеспечение с использованием криптографических средств защиты информации, в том числе ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), от несанкционированного доступа, подделки (несанкционированной модификации), а также обеспечение таких свойств информации, как неотказуемость, подотчётность, аутентичность.

# **2.** **Планируемые результаты обучения**

Процесс освоения обучающимися дополнительной профессиональной программы повышения квалификации направлен на **качественное изменение следующих компетенций**:

**общепрофессиональных:**

• способность понимать сущность и значение информации и её криптографической защиты в современном обществе, применять достижения информатики и вычислительной техники, перерабатывать большие объёмы информации, проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

• способность определять виды и формы информации, подверженной угрозам, виды, возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов, целей и задач деятельности организации;

**профессиональных:**

• способность использовать нормативно-правовые акты в своей профессиональной деятельности;

• способность формировать эффективный комплекс мер по безопасности информации с учётом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

• способность организовывать и поддерживать выполнение комплекса мер по безопасному использованию средств криптографической защиты информации, управлять процессом их реализации с учётом решаемых задач и организационной структуры предприятия, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации.

В процессе изучения программы решаются **задачи:**

• получение знаний об организационной структуре органов криптографической защиты информации в организациях;

• получение знаний о номенклатуре и характеристиках сертифицированных средств криптографической защиты информации;

• усвоение обучающимися необходимых условий для проведения мероприятий по криптографической защите информации;

• формирование навыков в выборе рационального состава средств криптографической защиты на конкретных автоматизированных рабочих местах в конкретных условиях эксплуатации, выполнения методов и процедур выявления нарушений безопасности криптографической защиты в организации, порядка осуществления работ по криптографической защите в организации;

• выработка практических рекомендаций и предложений по усилению эффективных мер, направленных на защиту конфиденциальной информации криптографическими средствами.

В результате освоения дополнительной профессиональной программы повышения квалификации обучающийся должен получить знания, умения и навыки, которые позволят качественно изменить соответствующие компетенции.

**Требования к компетентности обучающихся по итогам обучения**

После прохождения обучения **обучающиеся должны:**

**иметь представление:**

• об основных понятиях в области криптографической защиты информации;

• об угрозах и уязвимостях в безопасной эксплуатации средств криптографической защиты на автоматизированных рабочих местах в организации;

• о возможных последствиях реализации угроз безопасной эксплуатации средств криптографической защиты на автоматизированных рабочих местах в организации;

• о возможных каналах утечки защищаемой информации;

• о несанкционированном доступе к информации и программно-математическом воздействии на неё;

• о способах и средствах криптографической защиты информации, применяемых в организации;

• о номенклатуре средств криптографической защиты информации;

• о существующем порядке сертификации средств криптографической защиты;

**знать:**

• содержание нормативных и методических документов ФСБ России по вопросам, связанным с обеспечением криптографической защиты информации;

• методы и средства получения, обработки и передачи информации;

• содержание научно-технической и другой специальной литературы по криптографической защите информации;

• методы и процедуры выявления угроз безопасности информации на автоматизированных рабочих местах организации с установленными средствами криптографической защиты;

• угрозы безопасности защищаемой информации;

• организацию работ по криптографической защите информации в организации;

• организация системы сертификации средств защиты информации;

• общие сведения о сертификации средств криптографической защиты информации;

• инструкции по соблюдению режима проведения работ по криптографической защите;

• перечень наиболее применяемых в практике средств криптографической защиты, их характеристики по основному назначению;

• порядок оформления организационной, эксплуатационной и технической документации по криптографической защите;

• отечественный и зарубежный опыт в области криптографической защиты информации;

**уметь:**

• реализовывать требования нормативно-методических и руководящих документов с учётом особенностей функционирования организации, а также действующего законодательства по вопросам криптографической защиты информации;

• составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер криптографической защиты информации;

• определять потребность в средствах криптографической защиты информации, контролировать их поставку и использование;

**владеть навыками:**

• работы с нормативными правовыми актами в области криптографической защиты информации в организации;

• разработки схемы криптографической защиты информации организации;

• проведения работ, связанных с криптографической защитой информации и контролем её эффективности;

• планирования и организации проведения работ по криптографической защите информации на уровне автоматизированного рабочего места;

• проектирования, построения и эксплуатации системы криптографической защиты информации в организации;

• разработки необходимой документации для организации работ по криптографической защите информации в организации;

• проведения оценки уровня защищённости информации, защищаемой криптографическими средствами;

• проверки соответствия автоматизированных рабочих мест и развёрнутых на них средств криптографической защиты требованиям руководящих документов и их готовности к эксплуатации.

# **3. Требования к квалификации лиц, поступающих на обучение**

**Объектами профессиональной деятельности обучающихся являются:**

• методы, средства обеспечения защиты с использованием криптографических средств конфиденциальности и целостности информации, обрабатываемой в информационных системах;

• эксплуатация средств криптографической защиты информации;

• организация и управление криптографической защитой информации в организациях.

**Виды профессиональной деятельности обучающихся:**

• организационно-управленческая;

• эксплуатационная.

**Категории обучающихся:**

• работники руководящего звена организаций, ответственные за безопасность информации и организацию работ по защите информации;

• руководители подразделений технической защиты информации (или лица, на которых возложены такие функции), ответственные за проведение работ по криптографической защите информации и бесперебойную работу средств криптографической защиты;

• специалисты, ответственные за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам криптографической защиты информации;

• администраторы средств криптографической защиты информации, ответственные за их эксплуатационное сопровождение;

• пользователи средств криптографической защиты информации.

# **4. Форма обучения**

Дистанционная без отрыва от производства.

# **5.** **Учебно-тематический план дополнительной профессиональной программы повышения квалификации «Защита информации с использованием криптографических средств»**

| **№** | **Наименование разделов и тем** | **Часов** |
| --- | --- | --- |
|  | **Раздел 1.** Нормативно-правовые основы обеспечения защиты информации с использованием криптографических средств в Российской Федерации | 18 |
|  | Тема № 1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» | 1 |
|  | Тема № 2. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» | 1 |
|  | Тема № 3. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» | 1 |
|  | Тема № 4. Постановление Правительства РФ от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и теле-коммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)». | 1 |
|  | Тема № 5. Приказ ФАПСИ РФ от 13 июня 2001 г. № 152 (Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну) | 4 |
|  | Тема № 6. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» | 1 |
|  | Тема № 7. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» | 1 |
|  | Тема № 8. Приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи» | 1 |
|  | Тема № 9. Приказ ФСБ России от 6 мая 2019 г. № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» | 1 |
|  | Тема № 10. Приказ ФСБ России от 24 октября 2022 г. № 524 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» | 1 |
|  | Тема № 11. Система сертификации средств криптографической защиты. | 1 |
|  | **Самостоятельная подготовка по разделу № 1** | 3 |
|  | **Промежуточный зачёт по разделу 1** | 1 |
|  | **Раздел 2.** Теоретические основы криптографической защиты информации | 12 |
|  | Тема № 12. Основы криптографии. | 1 |
|  | Тема № 13. Применение шифрования информации в компьютерных системах и электронном документообороте | 1 |
|  | Тема № 14. Применение электронной подписи в компьютерных системах и электронном документообороте в условиях текущего нормативно-правового обеспечения | 3 |
|  | Тема № 15. Виды средств криптографической защиты информации и принципы их действия | 4 |
|  | **Самостоятельная подготовка по разделу № 2** | 3 |
|  | **Промежуточный зачёт по разделу 2** | 1 |
|  | **Раздел 3.** Организация применения средств криптографической защиты информации (СКЗИ) в организации | 15 |
|  | Тема № 16. Организационно-распорядительная документация по эксплуатации СКЗИ | 3 |
|  | Тема № 17. Оборудование помещений и рабочих мест, на которых эксплуатируются СКЗИ | 2 |
|  | Тема № 18. Эксплуатационная и техническая документация, сопровождающая применение СКЗИ, правила её ведения | 3 |
|  | Тема № 19. Ведение учёта СКЗИ и ключевых документов | 1 |
|  | Тема № 20. Обучение пользователей работе со средствами криптографической защиты | 1 |
|  | Тема № 21. Контроль за применением средств криптографической защиты в организации | 1 |
|  | **Самостоятельная подготовка по разделу № 3** | 3 |
|  | **Промежуточный зачёт по разделу 3** | 1 |
|  | **Раздел 4.** Эксплуатация распространённых программных СКЗИ на автоматизированных рабочих местах пользователей | 13 |
|  | Тема № 22. Общие требования по эксплуатации средств криптографической защиты информации | 4 |
|  | Тема № 23. Эксплуатация программного СКЗИ КриптоПро CSP | 2 |
|  | Тема № 24. Эксплуатация программного СКЗИ ViPNet CSP | 2 |
|  | Тема № 25. Эксплуатация программного СКЗИ ViPNet Client | 2 |
|  | **Самостоятельная подготовка по разделу № 4** | 2 |
|  | **Промежуточный контроль по разделу 4 (зачёт)** | 1 |
|  | **Лабораторная работа № 1.** Установка, применение, удаление СКЗИ КриптоПро CSP. Генерация ключа электронной подписи и запроса на получение сертификата в удостоверяющем центре | 2 |
|  | **Лабораторная работа № 2.** Установка, применение, удаление СКЗИ ViPNet CSP. Генерация ключа электронной подписи и запроса на получение сертификата в удостоверяющем центре | 2 |
|  | **Лабораторная работа № 3.** Установка, применение, удаление ПО СКЗИ ViPNet Client. Генерация запроса в УКЦ на получение и установка файла \*.dst | 2 |
|  | Подготовка к итоговой аттестации (самоподготовка, консультации) | 6 |
|  | **Итоговая аттестация** | 2 |
|  | **Всего на курс** | 72 |

# **6. Календарный учебный график**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Календарных дней** | | | **Распределение учебного времени (часы)** | | | | | |
| **всего** | **из них** | | **учебные занятия, всего** | **в том числе** | | **самостоятельная подготовка** | **промежуточный контроль** | **итоговая аттестация** |
| **учебных** | **выходных** | **изучение учебного материала** | **практика** |
| 12 | 10 | 2 | 72 | 44 | 6 | 16 | 4 | 2 |

# **7.** **Программы учебных тем**

**Раздел 1. Нормативно-правовые основы обеспечения защиты информации с использованием криптографических средств в Российской Федерации**

**Тема № 1.** Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Сфера действия настоящего Федерального закона.

Основные понятия, используемые в настоящем Федеральном законе.

Общедоступная информация.

Ограничение доступа к информации.

Соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Порядок доступа к персональным данным граждан (физических лиц).

Использование шифровальных (криптографических) средств при предоставлении биометрических персональных данных физического лица по каналам связи.

Защита информации.

Соблюдение конфиденциальности информации ограниченного доступа.

**Тема № 2.** Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Цель настоящего Федерального закона.

Основные понятия, используемые в настоящем Федеральном законе.

Конфиденциальность персональных данных.

Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом.

Меры по обеспечению безопасности персональных данных при их обработке.

Лица, ответственные за организацию обработки персональных данных в организациях.

**Тема № 3.** Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Система защиты персональных данных.

Выбор средств защиты информации для системы защиты персональных данных.

Актуальные угрозы безопасности персональных данных.

Уровни защищённости персональных данных.

Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

**Тема № 4.** Постановление Правительства РФ от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и теле-коммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

Лицензирование деятельности по криптографической защите информации.

Перечень средств, относящихся к шифровальным (криптографической защиты информации).

Перечень выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств.

Кем осуществляется лицензирование деятельности в отношении шифровальных (криптографических) средств.

Лицензионные требования при осуществлении лицензируемой деятельности.

Какие документы представляет в лицензирующий орган соискатель лицензии для получения лицензии.

Осуществление лицензионного контроля.

**Тема № 5.** Приказ ФАПСИ РФ от 13 июня 2001 г. № 152 (Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну).

Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации в сетях конфиденциальной связи и вне их.

Деятельность и ответственность лицензиатов ФСБ России.

Организация лицензиатами ФСБ России органов криптографической защиты.

Функции, осуществляемые органами криптографической защиты.

Обязанность обладателей конфиденциальной информации выполнять указания соответствующих органов криптографической защиты.

Условия допуска к выполнению обязанностей сотрудников органов криптографической защиты лицензиатами ФСБ России.

Чем обеспечивается безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

Кто имеет право на обучение и повышение квалификации сотрудников органов криптографической защиты.

Объём, содержание, распределение и утверждение лицензиатом ФСБ России функциональных обязанностей сотрудников органа криптографической защиты.

Допуск физических лиц к работе с СКЗИ.

Обязанности пользователей СКЗИ.

Обучение пользователей правилам работы с СКЗИ.

Порядок обращения с СКЗИ и криптоключами к ним.

Отнесение ключевых документов к материальным носителям, содержащим служебную информацию ограниченного распространения.

Порядок поэкземплярного учёта используемых или хранимых СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Ключевой носитель многократного использования как единица поэкземплярного учета ключевых документов.

Ведение журналов поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Выдача в пользование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. Ведение органами криптографической защиты лицевых счетов пользователей.

Хранение инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к СКЗИ, ключевых документов в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним.

Оборудование аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ средствами контроля за их вскрытием.

Доставка СКЗИ и ключевых документов. Правила упаковки.

Получение СКЗИ и ключевых документов в органах криптографической защиты. Подтверждение получения.

Сроки, порядок и оформление уничтожения криптоключей и ключевых носителей.

Уничтожение СКЗИ.

Что понимается под компрометацией криптоключей в настоящей Инструкции.

Мероприятия при компрометации криптоключей.

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним.

Требования к сохранности конфиденциальной информации, СКЗИ, ключевых документов.

Оборудование спецпомещений органов криптографической защиты с учётом размеров контролируемых зон.

Режим охраны спецпомещений органов криптографической защиты.

Допуск в спецпомещения органов криптографической защиты.

Внутренний режим в спецпомещениях органов криптографической защиты.

Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

Типовые формы журналов учёта.

**Тема № 6.** Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Предмет регулирования Положения.

Перечень видов средств, относящихся к СКЗИ.

Условия, при которых необходимо руководствоваться настоящим Положением.

Условия, при которых требования Положения носят рекомендательный характер.

На какие отношения не распространяются требования Положения.

Кем определяется выбор СКЗИ для защиты конфиденциальной информации.

Кем определяется необходимость защиты конфиденциальной информации.

Требования по безопасности информации, устанавливаемые в соответствии с законодательством Российской Федерации.

Порядок разработки СКЗИ.

Порядок производства СКЗИ.

Порядок реализации (распространения) СКЗИ.

Порядок эксплуатации СКЗИ.

Контроль за соблюдением правил пользования СКЗИ и условий их использования.

**Тема № 7.** Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Назначение документа.

Состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 4 уровня защищённости.

Состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 3 уровня защищённости.

Состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 2 уровня защищённости.

Состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 1 уровня защищённости.

**Тема № 8.** Приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Основание для разработки Требований.

Основные понятия, используемые в настоящих Требованиях.

Установление требований к совокупности и порядку расположения полей квалифицированного сертификата.

Содержание квалифицированного сертификата соответствует ст. 14 и 17 Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

Какой и чьей электронной подписью подписываются квалифицированные сертификаты.

Дополнительная информация о владельце квалифицированного сертификата.

Требования к порядку расположения полей квалифицированного сертификата.

Структура квалифицированного сертификата в форме электронного документа.

Содержание и формат полей квалифицированного сертификата.

Стандартные атрибуты имени (CN=) владельца сертификата, их формат и содержание.

Дополнительные атрибуты имени (CN=) владельца сертификата, их формат и содержание.

Использование необязательных полей и дополнительной информации (дополнений) в квалифицированном сертификате.

Применение объектных идентификаторов для обозначения класса средств электронной подписи владельца квалифицированного сертификата.

Указание в квалифицированном сертификате идентификатора, однозначно указывающего на способ идентификации заявителя при выдаче сертификата.

Указание в квалифицированном сертификате наименования используемого владельцем квалифицированного сертификата средства электронной подписи (ЭП).

Указание в квалифицированном сертификате наименования средств ЭП и средств аккредитованного УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, квалифицированного сертификата, а также реквизитов документа, подтверждающего соответствие указанных средств требованиям, установленным законодательством Российской Федерации.

Требования к форме квалифицированного сертификата на бумажном носителе.

Общий вид квалифицированного сертификата на бумажном носителе для владельцев – физических лиц, юридических лиц и индивидуальных предпринимателей (приложения №№ 1, 2, 3 к приказу).

**Тема № 9.** Приказ ФСБ России от 6 мая 2019 г. № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».

Требования к средствам обмена и криптографическим средствам защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

**Тема № 10.** Приказ ФСБ России от 24 октября 2022 г. № 524 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств».

Обязательность защиты информации, содержащейся в государственных информационных системах (ГИС), с использованием шифровальных (криптографических) средств.

Обоснование необходимости использования СКЗИ для защиты информации, содержащейся в ГИС, в модели угроз безопасности информации, техническом проекте и техническом задании на создание (развитие) ГИС.

Использование для обеспечения защиты информации, содержащейся в ГИС, только СКЗИ соответствующего класса, сертифицированных ФСБ России.

Оценка влияния среды функционирования на применяемые в ГИС СКЗИ. Согласование с ФСБ России.

Режим в помещениях, в которых размещены и (или) хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

Правила определения класса СКЗИ, подлежащих использованию для защиты информации, содержащейся в ГИС.

Использование таблицы в приложении к Требованиям для определения минимально допустимого класса СКЗИ, подлежащих использованию для защиты информации, содержащейся в ГИС (сегменте ГИС).

**Тема № 11.** Система сертификации средств криптографической защиты.

Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

Система сертификации средств защиты информации как совокупность участников сертификации, осуществляющих её по установленным правилам.

Координация работ по организации сертификации средств защиты информации.

Участники сертификации средств защиты информации.

Аккредитация органов по сертификации средств защиты информации.

Компетенция федерального органа по сертификации.

Компетенция центральных органов системы сертификации.

Компетенция органов по сертификации средств защиты информации.

Компетенция испытательных лабораторий и изготовителей средств защиты информации.

Порядок получения сертификатов соответствия изготовителями средств защиты информации.

Срок действия сертификатов соответствия.

Приостановка или аннулирование действия сертификатов.

Указ Президента Российской Федерации от 11 августа 2003 г. № 960 «Вопросы Федеральной службы безопасности Российской Федерации».

Функция ФСБ России по сертификации технических, программных и программно-технических средств защиты информации, включая средства контроля эффективности мер защиты информации, систем и комплексов телекоммуникаций, технических и программно-технических средств, используемых в целях выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах, а также сертификацию технических и программно-технических средств и систем в защищённом исполнении, защищённых программных средств обработки информации, шифровальных (криптографических) средств защиты информации.

**Раздел 2. Теоретические основы криптографической защиты информации**

**Тема № 12.** Основы криптографии.

Введение.

Краткий очерк из истории криптографии.

Основные понятия криптографии (криптография, конфиденциальность, целостность, аутентификация, цифровая подпись).

Инфраструктура открытых ключей (сертификаты, центры сертификации).

**Тема № 13.** Применение шифрования информации в компьютерных системах и электронном документообороте.

Основная задача шифрования – обеспечение конфиденциальности информации, передаваемой по каналам связи или хранимой на носителях, доступ к которым не защищён организационными мерами.

Угрозы безопасности защищаемой информации.

Принципы построения систем шифрования.

Управление закрытыми ключами.

Предварительное распределение ключей.

Пересылка ключей.

Открытое распределение ключей.

Схема разделения секрета.

**Тема № 14.** Применение электронной подписи в компьютерных системах и электронном документообороте в условиях текущего нормативно-правового обеспечения.

Основные термины (понятия).

Структура квалифицированного сертификата ключа проверки электронной подписи.

Назначение сертификата, распечатанного на бумажном носителе.

Безопасное использование электронной подписи.

Основные области применения квалифицированной электронной подписи.

Выбор криптопровайдера (СКЗИ).

Подписание электронных документов и проверка электронной подписи в электронных документах.

Основные процедуры по получению квалифицированных сертификатов ключа проверки электронной подписи.

О преступлениях с применением квалифицированных сертификатов и сформированных с их помощью электронных подписей.

Выдача квалифицированных сертификатов государственными удостоверяющими центрами.

**Тема № 15.** Средства криптографической защиты информации и принципы их действия.

Определение криптографических средств защиты информации.

Обзор средств криптографической защиты информации, сертифицированных ФСБ России.

Обзор сетей защищённой связи на базе решений АО «ИнфоТеКС» и ООО «Код Безопасности».

**Раздел 3. Организация применения средств криптографической защиты информации (СКЗИ) в организации**

**Тема № 16.** Организационно-распорядительная документация по эксплуатации СКЗИ в организации.

Распорядительный документ о назначении лица (лиц), ответственного за организацию безопасности информации.

Распорядительный документ о назначении лица (лиц), ответственного за реализацию мер по криптографической защите информации в организации.

Распорядительный документ о назначении лица (лиц), допущенного к использованию (эксплуатации) средств криптографической защиты.

Распорядительный документ об организации органа криптографической защиты, его структуре и утверждении положения об органе криптографической защиты.

Письменное уведомление ФСБ России о создании органа криптографической защиты.

Распорядительный документ об утверждении состава сотрудников органа криптографической защиты.

Распорядительный документ об утверждении перечня помещений, где размещены и/или хранятся используемые криптосредства и/или носители ключевой, аутентифицирующей и парольной информации.

Инструкция руководителю органа криптографической защиты.

Инструкция администратору безопасности средств криптографической защиты информации органа криптографической защиты.

Инструкция техническому специалисту органа криптографической защиты.

Инструкция пользователю средств криптографической защиты информации.

Инструкция о порядке действий пользователей средств криптографической защиты информации при компрометации криптографических ключей.

Порядок организации режима безопасности, предотвращения и ликвидации последствий чрезвычайных ситуаций в специальных помещениях органа криптографической защиты.

Положение (инструкция, порядок) об охране спецпомещений органа криптографической защиты.

Порядок уничтожения средств криптографической защиты информации и криптографических ключей к ним.

Схема организации криптографической защиты конфиденциальной информации органом криптографической защиты.

Список лиц, ознакомленных под расписку с Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утверждённой приказом ФАПСИ РФ от 13 июня 2001 г. № 152 (далее по тексту – Инструкция ФАПСИ № 152).

План мероприятий по обеспечению функционирования и безопасности применяемых СКЗИ.

План контроля за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ и Инструкцией ФАПСИ № 152.

Программа обучения лиц, использующих СКЗИ, правилам работы с ними.

Заключения о возможности эксплуатации СКЗИ организациями и пользователями.

Заключения о допуске лиц, ответственных за эксплуатацию СКЗИ, к самостоятельной работе с СКЗИ.

Списки лиц, имеющих право бесконтрольного нахождения в помещениях органа криптографической защиты и/или в помещениях с размещёнными там СКЗИ.

**Тема № 17.** Оборудование помещений и рабочих мест, на которых эксплуатируются СКЗИ.

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним.

Требования к средствам хранения конфиденциальной информации, СКЗИ, ключевых документов.

Оборудование спецпомещений органов криптографической защиты.

Режим охраны спецпомещений органов криптографической защиты.

Допуск в спецпомещения органов криптографической защиты.

Действия при возникновении чрезвычайных ситуаций в спецпомещении органа криптографической защиты или возле него.

Внутренний режим в спецпомещениях органов криптографической защиты.

**Тема № 18.** Эксплуатационная и техническая документация, сопровождающая применение СКЗИ, правила её ведения.

Формуляры (паспорта) средств криптографической защиты.

Руководства разработчиков СКЗИ.

Руководства по эксплуатации СКЗИ для администраторов и пользователей.

Правила пользования СКЗИ.

Лицензии и сертификаты на СКЗИ.

**Тема № 19.** Ведение учёта СКЗИ и ключевых документов.

Журнал поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для органа криптографической защиты или для обладателя конфиденциальной информации).

Журнал учёта обучения лиц, использующих СКЗИ, правилам работы с ними.

Заключения по итогам обучения сотрудников (должностных лиц) правилам работы с СКЗИ.

Лицевые счета на СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы.

Реестры на отправленные СКЗИ и ключевые документы.

Акты об уничтожении СКЗИ или ключевых документов.

Журнал учёта книг, изданий, журналов и неподшитых в дела документов органа криптографической защиты.

Журнал учёта сейфов (хранилищ) и ключей от спецпомещений органа криптографической защиты.

Журнал учёта выдачи и возврата ключей от помещений и хранилищ.

Журнал учёта печатей и штампов.

**Тема № 20.** Обучение пользователей работе со средствами криптографической защиты.

Организация обучения пользователей работе со СКЗИ.

Программа подготовки пользователей к работе со СКЗИ.

Формы итоговой аттестации и контроля.

Порядок допуска пользователей к самостоятельной работе с СКЗИ.

**Тема № 21.** Контроль за применением средств криптографической защиты.

Плановый и внеплановый государственный контроль деятельности лицензиатов ФСБ России.

Документы по результатам проверок и порядок устранения отмеченных нарушений и недостатков.

Условия отзыва (приостановления действия) лицензий ФСБ России.

Контроль лицензиатами ФСБ России (органами криптографической защиты) выполнения обладателями конфиденциальной информации данных им указаний по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, а также соблюдение такими обладателями условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФСБ России и Инструкцией ФАПСИ № 152.

Обобщение результатов всех видов контроля, анализ причин выявленных недостатков, разработка мер по их профилактике, контроль выполнения рекомендаций, содержащихся в актах проверок.

**Раздел 4. Эксплуатация распространённых программных СКЗИ на автоматизированных рабочих местах пользователей**

**Тема № 22.** Общие требования по эксплуатации средств криптографической защиты информации.

Установка аппаратных и программных СКЗИ.

Эксплуатационные возможности СКЗИ.

Применение СКЗИ в ходе эксплуатации.

Порядок вывода из эксплуатации и утилизации СКЗИ.

**Тема № 23.** Эксплуатация программного СКЗИ КриптоПро CSP.

Назначение СКЗИ КриптоПро CSP.

Условия эксплуатации СКЗИ КриптоПро CSP согласно формуляру.

Установка программного СКЗИ КриптоПро CSP.

Ввод лицензионного номера (ключа), использование специальных объектных идентификаторов (OID) в квалифицированных сертификатах для активации лицензионного использования программного продукта.

Использование СКЗИ КриптоПро CSP для шифрования или дешифрования информации (файлов), подписания информации (файлов) электронной подписью или проверки подлинности электронной подписи.

Деинсталляция программного обеспечения СКЗИ КриптоПро CSP.

**Тема № 24.** Эксплуатация программного СКЗИ ViPNet CSP.

Назначение СКЗИ ViPNet CSP.

Условия эксплуатации СКЗИ ViPNet CSP согласно формуляру.

Установка программного СКЗИ ViPNet CSP.

Особенности получения лицензии на программное СКЗИ ViPNet CSP.

Использование СКЗИ ViPNet CSP для шифрования или дешифрования информации (файлов), подписания информации (файлов) электронной подписью или проверки подлинности электронной подписи

Деинсталляция программного СКЗИ ViPNet CSP.

**Тема № 25.** Эксплуатация программного СКЗИ ViPNet Client.

Назначение программного обеспечения ViPNet Client.

Состав компонентов программного обеспечения ViPNet Client.

Условия эксплуатации СКЗИ ViPNet Client согласно формуляру.

Установка программного СКЗИ ViPNet Client.

Особенности получения лицензии на программное СКЗИ ViPNet Client.

Получение и установка файла (формата \*.dst) с криптоключом, конфигурацией и лицензией.

Использование некоторых функций СКЗИ ViPNet Client.

Деинсталляция программного СКЗИ ViPNet Client.

# **8. Условия реализации программы**

Подготовка слушателей по учебной программе направлена на повышение их квалификации по вопросам защиты информации криптографическими средствами в соответствии с требованиями законодательства Российской Федерации и иных нормативно-правовых актов.

В ходе изучения программы используются правовые, организационно-распорядительные и нормативные документы в области криптографической защиты информации, учебно-методические пособия, иллюстративные материалы (презентации). Для изучения учебного материала и контроля знаний на основе тестирования используются различные формы дистанционного обучения.

Практические занятия обеспечиваются лабораторными практикумами. При проведении практических занятий проводится отработка заданий, учитывающих специфику выполняемых функциональных обязанностей слушателей курсов, в том числе с проработкой реальных ситуаций, возникающих в процессе построения системы криптографической защиты.

На самостоятельное изучение учебного материала отведено 16 академических часов. Для самостоятельной работы слушатели курсов получают задания от преподавателя по углубленному изучению тем курса. Данный вид работы направлен на развитие активности слушателей, учит их самостоятельно анализировать и объективно оценивать сущность вопроса, проблемы.

Изменение наименования учебной программы утверждается распорядительным актом (приказом) директора СОГАУ «ЦИТ» после согласования с региональным Управлением ФСБ России. Об изменении наименования учебной программы в лицензирующий орган направляется заявление о внесении изменений в реестр лицензий с приложением копии новой редакции программы.

# **9. Форма аттестации**

Для оценки качества обучения и контроля знаний, навыков и умений, полученных слушателями в процессе повышения квалификации, по итогам обучения проводится итоговая аттестация.

В качестве итоговой формы контроля проводится сертификационный экзамен (тест), являющийся заключительным этапом изучения настоящей учебной программы и имеющий целью проверить и оценить уровень полученных знаний, навыки и умения применить полученные знания в решении практических задач.

# **10.** **Оценочные материалы**

| **№** | **Тема (раздел)** | **Оценочный материал** | **Форма фиксации результатов** |
| --- | --- | --- | --- |
|  | Раздел 1. Темы №№ 1÷11 | Промежуточный зачёт по разделу (тест) | Таблица № 1 (результаты освоения раздела 1 программы) |
|  | Раздел 2. Темы №№ 12÷15 | Промежуточный зачёт по разделу (тест) | Таблица № 2 (результаты освоения раздела 2 программы) |
|  | Раздел 3. Темы №№ 16÷21 | Промежуточный зачёт по разделу (тест) | Таблица № 3 (результаты освоения раздела 3 программы) |
|  | Раздел 4. Темы №№ 22÷25 | Промежуточный зачёт по разделу (тест) | Таблица № 4 (результаты освоения раздела 4 программы) |
|  | Разделы 1÷4 | Итоговая аттестация (тест) | Таблица № 5 (результаты освоения дополнительной образовательной программы) |

Таблица № 1

| **№** | **Вопросы** | **Ответы** | **Правильные**  **ответы** |
| --- | --- | --- | --- |
|  | Что такое конфиденциальность информации согласно Федеральному закону от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»? | 1) возможность получения информации и её использования  2) обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя  3) получение информации определённым кругом лиц  4) передача информации определённому кругу лиц  5) получение информации неопределённым кругом лиц  6) передача информации неопределённому кругу лиц | один (2) |
|  | Что из перечисленного **не** **является** функциями органа криптографической защиты (согласно Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ с ограниченным доступом, утв. приказом ФАПСИ от 13.06.2001 № 152)? | 1) проверка готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ  2) обучение лиц, использующих СКЗИ, правилам работы с ними  3) поэкземплярный учёт используемых СКЗИ, эксплуатационной и технической документации к ним  4) учёт и внедрение средств защиты информации от несанкционированного доступа к ней  5) контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ  6) расследование и составление заключений по фактам нарушения условий использования СКЗИ | один (4) |
|  | Что из перечисленного **не** является обязанностью пользователей СКЗИ (согласно Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ с ограниченным доступом, утв. приказом ФАПСИ от 13.06.2001 № 152)? | 1) не разглашать конфиденциальную информацию, к которой они допущены, в том числе сведения о криптоключах  2) соблюдать правила трудового распорядка и охраны труда на рабочем месте  3) соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ  4) вести поэкземплярный учёт СКЗИ и ключевой документации к ним  5) немедленно уведомлять орган криптозащиты об утрате или недостаче СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей  6) сообщать в орган криптозащиты о попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним  7) сдать СКЗИ, документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ | два (2, 4) |
|  | Какая информация **не** должна содержаться в квалифицированном сертификате (согласно приказу ФСБ России от 27.12.2011 № 795)? | 1) уникальный номер сертификата  2) даты начала и окончания действия сертификата  3) фамилия, имя и отчество владельца сертификата - для физического лица  4) ключ проверки электронной подписи  5) наименование используемого средства ЭП  6) идентификационный номер налогоплательщика владельца сертификата – для юридического лица  7) наименование и место нахождения аккредитованного УЦ, который выдал сертификат  8) ограничения использования сертификата  9) квалифицированная ЭП аккредитованного УЦ  10) нет правильного ответа | один (10) |
|  | Уполномоченными органами Российской Федерации по сертификации средств криптографической защиты информации являются: | 1) Министерство обороны РФ  2) ФСТЭК России  3) ФСБ России  4) Федеральное агентство по техническому регулированию и метрологии  5) Министерство цифрового развития, связи и массовых коммуникаций РФ  6) ни один из перечисленных органов | один (3) |

Таблица № 2

| **№** | **Вопросы** | **Ответы** | **Правильные**  **ответы** |
| --- | --- | --- | --- |
|  | Что такое современная криптография? | 1) часть деятельности по обеспечению безопасности информации  2) использование нестандартных способов передачи сообщений для сокрытия канала передачи информации  3) область знаний, связанная с обеспечением таких свойств информации, как конфиденциальность, целостность, аутентификация и невозможность отказа сторон от авторства  4) маскировка канала передачи закрытой информации в открытом канале связи  5) существенное затруднение возможности перехвата про­тивником передаваемых сообщений с использованием специальных методов передачи по широкополосным каналам сигнала под уровнем шумов, либо с использованием «прыгающих» несущих частот и т.п. | два (1, 3) |
|  | Какими криптографическими методами обеспечивается конфиденциальность информации? | 1) цифровая подпись  2) формирование имитовставки  3) шифрование  4) расшифрование  5) всё перечисленное в п.п. 1÷4 | один (3) |
|  | Какие криптографические методы используются для обеспечения невозможности отказа от авторства? | 1) расшифрование  2) формирование имитовставки  3) шифрование  4) цифровая подпись  5) всё перечисленное в п.п. 1÷4 | один (4) |
|  | Что такое сертификат открытого ключа? | 1) набор данных, заверенный цифровой подписью Центра сертификации,  2) набор данных, включающий открытый ключ  3) набор данных, включающий закрытый ключ шифрования и электронной подписи 4) набор данных, включающий список дополнительных атрибутов, принадлежащих абоненту (имена пользователя и Центра сертификации, номер сертификата, срок действия сертификата, предназначение открытого ключа)  5) набор данных, общую структуру которого определяет Международный стандарт ISO Х.509 | четыре (1, 2, 4, 5) |
|  | Для чего предназначены Центры сертификации? | 1) изготовление сертификатов открытых ключей  2) выпуск списка досрочно отозванных сертификатов  3) регистрация абонентов  4) хранение изготовленных сертификатов  5) поддержание в актуальном состоянии справочника действующих сертификатов  6) ничего из перечисленного в п.п. 1÷5 | пять (1, 2, 3, 4, 5) |

Таблица № 3

| **№** | **Вопросы** | **Ответы** | **Правильные**  **ответы** |
| --- | --- | --- | --- |
|  | Определение ключевого документа согласно Инструкции № 152: | 1) флэш-накопитель  2) физический носитель определённой структуры, содержащий ключевую информацию  3) документ, в котором изложены правила использования криптоключей  4) документ, в котором учитываются криптоключи | один (2) |
|  | Какое оборудование **не** является обязательным для спецпомещений органов криптографической защиты и тех, где размещены СКЗИ и ключевые документы? | 1) прочные входные двери с замками, гарантирующими надёжное закрытие помещений  2) металлические решетки или ставни на окнах первых и последних этажей  3) печи для сжигания документов, содержащих конфиденциальную информацию  4) кондиционеры воздуха  5) шторы на окнах | два (3,4) |
|  | Какие документы относятся к эксплуатационным для СКЗИ? | 1) Формуляры (паспорта) средств криптографической защиты  2) Руководства разработчиков СКЗИ (программистов)  3) Руководства по эксплуатации СКЗИ для администраторов и пользователей  4) Правила пользования СКЗИ  5) Лицензии и сертификаты на СКЗИ  6) Документы, перечисленные в п.п. 1÷4 | пять (1, 2, 3, 4, 5) |
|  | Подлежат ли сертификации ФСБ России формуляры (паспорта) средств криптографической защиты информации? | 1) да  2) нет  3) только для СКЗИ, предназначенных для защиты информации, содержащей государственную тайну | один (1) |
|  | Кем ведутся Журналы поэкземплярного учёта средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов? | 1) пользователями СКЗИ на рабочих местах  2) органами криптографической защиты  3) обладателями конфиденциальной информации  4) бухгалтерскими подразделениями учреждений  5) органами ФСБ России | два (2, 3) |

Таблица № 4

| **№** | **Вопросы** | **Ответы** | **Правильные**  **ответы** |
| --- | --- | --- | --- |
|  | К эксплуатационным возможностям СКЗИ относятся: | 1) вычисление и проверка электронной подписи  2) создание сертификатов открытых ключей  3) генерация ключей электронной подписи, ключей проверки электронной подписи и ключей шифрования  4) приём и отправка зашифрованных сообщений  5) вычисление хеш-функции  6) выработка случайных и псевдослучайных чисел, сессионных ключей шифрования | четыре (1, 3, 5, 6) |
|  | После удаления программы СКЗИ КриптоПро CSP следует **обязательно**: | 1) переустановить операционную систему Windows  2) уничтожить бумажный носитель с лицензией на программное обеспечение СКЗИ  3) перезагрузить компьютер  4) произвести очистку реестра операционные системы Windows | один (3) |
|  | Регистрация СКЗИ ViPNet CSP может производиться: | 1) до или после истечения ознакомительного срока с помощью функции регистрации программы  2) при установке программы, в т.ч. в автоматическом режиме  3) с использованием телефонной связи с АО «ИнфоТеКС»  4) с использованием сообщений электронной почты  5) с использованием почтовой (фельдъегерской) связи  6) через Интернет (online) | пять (1, 2, 3, 4, 6) |
|  | Какие из перечисленных компонентов **не** входят в программный комплекс ViPNet Client? | 1) низкоуровневый драйвер сетевой защиты (ViPNet-драйвер)  2) программа ViPNet Монитор  3) программа ViPNet Coordinator  4) транспортный модуль ViPNet MFTP  5) программа ViPNet Контроль приложений  6) программа ViPNet Деловая почта  7) криптопровайдер ViPNet CSP  8) программа ViPNet Удостоверяющий и ключевой центр | шесть (1, 2, 4, 5, 6, 7) |
|  | Автопроцессинг программы ViPNet Деловая почта реализует автоматизированные функции: | 1) отправка подтверждений прочтения входящих писем  2) отправка формализованных ответов на входящие сообщения  3) обработка входящих писем (извлечение в заданную папку вложенных файлов)  4) обработка исходящих файлов (отправка в заданные адреса исходящих сообщений с вложенными файлами из заданных папок) | три (1, 3, 4) |

Таблица № 5

| **№** | **Вопросы** | **Ответы** | **Правильные**  **ответы** |
| --- | --- | --- | --- |
|  | Чем устанавливаются условия отнесения информации к сведениям, составляющим коммерческую, служебную и иную тайны, обязательность соблюдения конфиденциальности такой информации, а также ответственность за её разглашение? | 1) постановлениями Правительства Российской Федерации и органов региональной исполнительной власти  2) соглашениями (договорами) сторон - участников информационного обмена  3) федеральными законами  4) распорядительными документами владельцев информации  5) приказами ФСТЭК России  6) решениями судебных органов РФ  7) ничем не устанавливаются | один (3) |
|  | Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: | 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;  2) соблюдение конфиденциальности информации ограниченного доступа;  3) реализацию права на свободный доступ неограниченного круга лиц к информации. | два (1, 2) |
|  | Каким требованиям должен удовлетворять квалифицированный сертификат согласно приказу ФСБ России от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»? | 1) быть созданным аккредитованным УЦ либо уполномоченным федеральным органом, и являться в связи с этим официальным документом  2) в сертификате должен быть идентификатор, однозначно указывающий, каким образом проводилась идентификация заявителя при выдаче сертификата  3) требованиям, установленным Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами  4) класс средства электронной подписи владельца сертификата, указанный в сертификате, должен быть не ниже КС3 | три (1, 2, 3) |
|  | Что является мерами по обеспечению безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн)? | 1) определение угроз безопасности ПДн при их обработке в ИСПДн  2) применение организационных и технических мер по обеспечению безопасности ПДн при их обработке, необходимых для выполнения требований к их защите  3) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации  4) оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн  5) учёт машинных носителей ПДн  6) обнаружение фактов несанкционированного доступа к ПДн и принятие мер по обнаружению, предупреждению и ликвидации последствий атак на ПДн  7) восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним  8) установление правил доступа к ПДн, обеспечение регистрации и учёта всех действий, совершаемых с ПДн в ИСПДн  9) контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищённости ИСПДн | девять (1, 2, 3, 4, 5, 6, 7, 8, 9) |
|  | Квалифицированная электронная подпись – это: | 1) сформированная сотрудником, имеющим на то все положенные полномочия  2) сформированная сотрудником, имеющим должную квалификацию для применения средств электронной подписи  3) полученная с помощью сертификата, содержащего в себе метку штампа времени подписания  4) полученная с помощью сертификата, действующего на момент проверки этой электронной подписи  5) полученная с помощью квалифицированного сертификата, выданного аккредитованным УЦ  6) действующая на момент её проверки  7) сформированная с применением логина и пароля пользователя | один (5) |
|  | Основными задачами при осуществлении режима охраны спецпомещений органов криптографической защиты являются: | 1) специальное оборудование спецпомещения защитными конструкциями, техническими средствами и имуществом, препятствующими силовому или неконтролируемому проникновению внутрь  2) ограничение доступа посетителей в спецпомещение  3) регулирование доступа персонала в спецпомещение организационными и техническими мерами  4) исключение техническими мерами свободного просмотра посторонними лицами ведущихся в спецпомещении работ  5) отработка взаимодействия с коммунальными службами и службами поддержания правопорядка по вопросам, связанным с безопасностью ОКЗ, ликвидацией последствий ЧС или угроз их наступления  6) поддержание инженерных (коммунальных) систем, находящихся в спецпомещении, в исправном состоянии, организация своевременного текущего или капитального ремонта неисправных систем (устройств)  7) оценка ущерба помещению, его оборудованию, аппаратным и программным средствам, конфиденциальности ключевой информации при наступлении чрезвычайных ситуаций или реализации несанкционированного проникновения в спецпомещение и выработка мер по ликвидации этого ущерба | семь (1, 2, 3, 4, 5, 6, 7) |
|  | С решением каких проблем безопасности информации связана современная криптография как область знаний? | 1) аутентификация  2) конфиденциальность  3) невозможность отказа сторон от авторства  4) целостность  5) ничего из перечисленного в п.п. 1÷4 | четыре (1, 2, 3, 4) |
|  | Шифрование информации в зависимости от структуры ключей, используемых при этом, делится на: | 1) гарантированной криптостойкости  2) временно́й криптостойкости  3) асимметричное  4) симметричное | два (3, 4) |
|  | Квалифицированная электронная подпись – это: | 1) сформированная сотрудником, имеющим на то все положенные полномочия  2) сформированная сотрудником, имеющим должную квалификацию для применения средств электронной подписи  3) полученная с помощью сертификата, содержащего в себе метку штампа времени подписания  4) полученная с помощью сертификата, действующего на момент проверки этой электронной подписи  5) полученная с помощью квалифицированного сертификата, выданного аккредитованным УЦ  6) действующая на момент её проверки  7) сформированная с применением логина и пароля пользователя | один (5) |
|  | Какие из перечисленных программ являются криптопровайдерами? | 1) КриптоАРМ  2) ViPNet CSP  3) КриптоПро CSP  4) ViPNet Coordinator  5) Код Безопасности CSP  6) ЭЦП Browser Plug-in  7) ViPNet Client  8) ViPNet Administrator | три (2, 3, 5) |
|  | Какие программы из состава линейки ViPNet CUSTOM относятся к **сетевым узлам** сети защищённой связи ViPNet? | 1) ViPNet Coordinator  2) ViPNet CSP  3) ViPNet Центр управления сетью  4) ViPNet Удостоверяющий и ключевой центр  5) ViPNet Client  6) ViPNet Administrator  7) ViPNet Registration Point | два (1, 5) |
|  | Что из перечисленного согласно Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утверждена приказом ФАПСИ РФ от 13 июня 2001 г. № 152) осуществляют органы криптографической защиты? | 1) поэкземплярный учёт используемых СКЗИ, эксплуатационной и технической документации к ним  2) выдачу лицензий обладателям конфиденциальной информации на применение СКЗИ  3) ремонт аппаратных СКЗИ и устранение неполадок в работе программных СКЗИ  4) обучение лиц, использующих СКЗИ, правилам работы с ними  5) разработку схемы организации криптографической защиты конфиденциальной информации  6) ничего из перечисленного не осуществляют | три (1, 4, 5) |

# **11.** **Список литературы**

**Нормативно-правовые акты**

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»
3. Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
4. Постановление Правительства РФ от 16.04.2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и теле-коммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».
5. Приказ ФАПСИ РФ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
6. Приказ ФСБ России от 09.02.2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»
7. Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
8. Приказ ФСБ России от 27.12.2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»
9. Приказ ФСБ России от 06.05.2019 г. № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»
10. Приказ ФСБ России от 24.10.2022 г. № 524 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств»
11. Постановление Правительства Российской Федерации от 26.06.1995 г. № 608 «О сертификации средств защиты информации».
12. Указ Президента Российской Федерации от 11.08.2003 г. № 960 «Вопросы Федеральной службы безопасности Российской Федерации».
13. Приказ Минобрнауки от 19.10.2020 г. № 1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности».

**Учебные и методические пособия**

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2001.
2. Осипян В.О., Осипян К.В. Криптография в задачах и упражнениях. – М.: Гелиос АРВ, 2004.
3. Файстель Хорст. Криптография и компьютерная безопасность: Статья. Перевод А. Винокурова. Перевод выполнен по изданию: Horst Feistel, Cryptography and Computer Privacy, Scientific American, May 1973, Vol. 228, No. 5, pp. 15-23.
4. С. Баричев, Р. Серов. Основы современной криптографии. – М.: Горячая линия – Телеком, 2001.
5. Бутакова Н.Г., Федоров Н.В. Криптографические методы и средства защиты информации: учебное пособие. − СПб.: ИЦ «Интермедия», 2019.
6. Воробейкина И. В. Методы и средства криптографической защиты информации: Учебно-методическое пособие – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022.
7. Салий В.Н. Криптографические методы и средства защиты информации: Учебное пособие – Саратов, 2017.
8. Коржук В.М., Попов И.Ю., Воробьева А.А. Защищенный документооборот. Часть 1: Учебно-методическое пособие – СПб: Университет ИТМО, 2021.
9. Кабакова Н.В., Чефранова А.О., Уривский А.В., Алабина Ю.Ф. Система защиты информации ViPNet: Учебное пособие – М: ДМК Пресс, 2014.
10. Чефранова А. О., Кабакова Н. В., Алабина Ю. Ф. Система защиты информации ViPNet: Практикум – М: Горячая линия - Телеком, 2015.
11. ViPNet Client 4. Руководство пользователя. ФРКЕ.00116-05 34 01 – М: АО «ИнфоТеКС», 2020.
12. Программный комплекс ViPNet Client 4. Версия 4.5. Правила пользования. ФРКЕ.00116-05 99 01 ПП – М: АО «ИнфоТеКС», 2020.
13. ViPNet CSP 4.4. Руководство пользователя. ФРКЕ.00106-07 34 01 – М: АО «ИнфоТеКС», 2021.
14. Средство криптографической защиты информации ViPNet CSP 4.4. Версия 4.4.2. Правила пользования. ФРКЕ.00106‑07 99 01 ПП – М: АО «ИнфоТеКС», 2021.
15. Средство криптографической защиты информации ViPNet CSP 4.4. Версия 4.4.2. Формуляр. ФРКЕ.00106-07 30 01 ФО – М: АО «ИнфоТеКС», 2021.
16. Средство криптографической защиты информации «КриптоПро CSP». Версия 5.0 R3 KC2. Исполнение 2-Base. Формуляр. ЖТЯИ.00102-03 30 01 – М: ООО «КРИПТО-ПРО», 2022.
17. Средство криптографической защиты информации. КриптоПро CSP. Версия 5.0 R3 KC2. Исполнение 2-Base. Правила пользования. ЖТЯИ.00102-03 95 01 – М: ООО «КРИПТО-ПРО», 2022.
18. Средство криптографической защиты информации. КриптоПро CSP. Версия 5.0 R3 KC2. Исполнение 2-Base. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows. ЖТЯИ.00102-03 91 02 – М: ООО «КРИПТО-ПРО», 2022.
19. Средство криптографической защиты информации. КриптоПро CSP. Версия 5.0 R3 KC2. Исполнение 2-Base. Инструкция по использованию СКЗИ под управлением ОС Windows. ЖТЯИ.00102-03 92 01 – М: ООО «КРИПТО-ПРО», 2022.
20. Комплекс безопасности Континент. Версия 4. Руководство администратора. Принципы функционирования. АМБС.26.20.40.140.001 90 1 – М: ООО «Код Безопасности», 2022.
21. Средство криптографической защиты информации Континент-АП. Версия 3.7. Руководство администратора. Windows. RU.88338853.501430.007 91 – М: ООО «Код Безопасности», 2022.
22. Методические рекомендации по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну – Смоленск: Комиссия по информационной безопасности при Администрации Смоленской области, Управление информационной безопасности смоленского областного государственного автономного учреждения «Центр информационных технологий», 2017.