

1. **Паспорт Образовательной программы**

**«**Способы и средства защиты информации от несанкционированного доступа в условиях цифровой трансформации **»**

|  |  |
| --- | --- |
| **Версия программы** | 1 |
| **Дата Версии** | **15.**10**.2020** |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | СКФУ |
| 1.2 | Логотип образовательной организации | Голосование |
| 1.3 | Провайдер ИНН | ИНН 2635014955 |
| 1.4 | Ответственный за программу ФИО | Чипига Александр Федорович |
| 1.5 | Ответственный должность | Заведующий кафедрой информационной безопасности автоматизированных систем Северо-Кавказского федерального университета |
| 1.6 | Ответственный Телефон | +79624007663 |
| 1.7 | Ответственный Е-mail | Chipiga.alexander@gmail.com |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Способы и средства защиты информации от несанкционированного доступа в условиях цифровой трансформации |
| 2.2 | Ссылка на страницу программы | [**https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/Sposoby-i-sredstva-zaity-informacii-ot-nesankcionirovannogo-dostupa-v-usloviyah-cifrovoi-transformacii/#**](https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/Sposoby-i-sredstva-zaity-informacii-ot-nesankcionirovannogo-dostupa-v-usloviyah-cifrovoi-transformacii/) |
| 2.3 | Формат обучения | Онлайн |
|  | Подтверждение от ОО наличия возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа | имеется |
| 2.4 | Уровень сложности | Продвинутый |
| 2.5 | Количество академических часов | **72** |
|  | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | 12 часов лекции, 24 часа практические занятия, 36 часов самостоятельная работа под руководством преподавателя, включая зачет |
| 2.6 | Стоимость обучения одного обучающегося по образовательной программе, а также предоставление ссылок на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости или обоснование уникальности представленной образовательной программы в случае отсутствия аналогичных образовательных программ на рынке образовательных услуг | 30000 рублей  <https://edu.softline.com/vendors/softline/tehnicheskaya-zashhita-informacii-sposoby-i-sredstva-zashhity-informacii-ot-nesankcionirovannogo-dostupa/>  <https://uc-echelon.ru/nashi-kursy/soglasovannye-fstek-rossii/tehnicheskaya-zashhita-informatsii-sposoby-i-sredstva-zashhity-informatsii-ot-nesanktsionirovannogo-dostupa/>  <https://www.academyit.ru/courses/%D0%A2%D0%97%D0%9A%D0%98013/> |
| 2.7 | Минимальное количество человек на курсе | 10 |
| 2.8 | Максимальное количество человек на курсе | Не ограничено |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | При наличии |
| 2.10 | Формы аттестации | Зачет |
|  | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Кибербезопасность и защита данных |

1. **Аннотация программы**

Наиболее полное и содержательное описание программы, которое включает:

1) общую характеристику компетенций, качественное изменение которых осуществляется в результате обучения или которые формируются в результате освоения образовательной программы;

2) описание требований и рекомендаций для обучения по образовательной программе;

3) краткое описание результатов обучения в свободной форме, а также описание востребованности результатов обучения в профессиональной деятельности.

Ограничение по размеру: не менее 1000 символов -?

Способы и средства защиты информации от несанкционированного доступа в условиях цифровой трансформации – практико-ориентированная дополнительная программа повышения квалификации, нацеленная на углубление знаний и формирование практических умений, навыков, а также приобретение опыта, необходимого для выполнения важного вида профессиональной деятельности в государственном секторе экономики (Техническая защиты информации) в части защиты информации государственных информационных систем в области цифровой экономики и соответствует области 5 «Кибербезопасность и защита данных».

Процесс освоения обучающимися программы повышения квалификации направлен на совершенствование следующих профессиональных компетенций:

способность формировать требования по технической защите информации (ТЗИ) от несанкционированного доступа (НСД) на объектах информатизации (формировать требования к системе защиты информации объекта информатизации;

способность внедрять способы и средства ТЗИ от НСД на объектах информатизации (внедрять системы защиты информации объекта информатизации;

способность обеспечивать ТЗИ от НСД в ходе эксплуатации объектов информатизации.

К освоению программы допускаются лица, имеющие среднее профессиональное или высшее образование по направлению подготовки (специальности) в области информационной безопасности, математических и естественных наук, инженерного дела, технологий и технических наук, подтвержденное документом об образовании, показавшие достаточные для усвоения программы знания в процессе входного контроля.

В результате освоения программы повышения квалификации, обучающиеся должны получить знания, умения и навыки, обеспечивающие совершенствование или получение новых компетенций, необходимых им для осуществления своей профессиональной деятельности и продвижения по службе.

Результаты освоения программы будут использоваться для повышения производительности труда и стимулирования личностного и профессионального роста, так как позволят слушателям демонстрировать профессионализм и высокий уровень квалификации в интересах развития карьеры, формировать индивидуальный цифровой профиль в рамках участия в цифровой трансформации.

В соответствии с моделью компетенций команды цифровой трансформации в системе государственного управления обучение по программе позволит освоить характеристику П.5.4 профессиональной компетенции П.5 в сфере цифрового развития: знания, умения и навыки применения средств и методов информационной и кибербезопасности.



**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Цель реализации программы повышения квалификации: совершенствование или получение новых компетенций, необходимых для осуществления профессиональной деятельности, или повышение профессионального уровня в рамках имеющейся квалификации специалистов (включая государственных гражданских служащих), работающих в области технической защиты информации (ТЗИ), в части внедрения и эксплуатации способов и средств защиты информации от несанкционированного доступа (НСД), в рамках профессиональной компетенции в сфере цифрового развития П.5 (Применение цифровых технологий), что позволит получить знания, умения и навыки применения средств и методов информационной и кибербезопасности в системе государственного управления.

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

2.1.1. нормативные правовые акты Российской Федерации, нормативные и методические документы в области ТЗИ (защиты информации от НСД);

2.1.2. основные понятия в области ТЗИ;

2.1.3. порядок проведения работ по сертификации средств защиты информации по требованиям безопасности информации;

2.1.4. систему организации защиты информации, действующей в органе государственной власти, организации;

2.1.5. основы методологии и методики проведения ТЗИ от НСД в органе государственной власти, организации;

2.1.6. процедуры выявления угроз безопасности информации на объектах информатизации, организации;

2.1.7. общие требования по ТЗИ (по защите информации от НСД), требования и рекомендации по защите объектов информатизации;

2.1.9. способы и средства защиты информации от НСД;

2.1.10. требования к средствам защиты информации от НСД;

2.1.11. цели, задачи, основные принципы организации, методы и средства ведения контроля состояния защищенности информации в органе государственной власти, организации;

2.1.12. порядок оформления технической документации по защите информации.

2.2. Умение (способность к деятельности)

2.2.1. анализировать угрозы безопасности информации;

2.2.2. определять требования к средствам защиты информации от НСД;

2.2.3. проводить обоснование выбора современных способов и средств защиты информации от НСД;

2.2.4. проводить мероприятия по защите информации от НСД;

2.2.5. устанавливать, применять и настраивать средства защиты информации от НСД;

2.2.6. разрабатывать проекты нормативных и методических документов по защите объектов информатизации от НСД к информации;

2.2.7. осуществлять проверку выполнения требований нормативных документов по защите информации от НСД;

2.2.8. осуществлять контроль защищенности информации от НСД.

2.3.Навыки (использование конкретных инструментов)

2.3.1 работы с нормативными правовыми актами, методическими документами, национальными и международными стандартами в области ТЗИ;

2.3.2. работы с базами данных, содержащих информацию по угрозам и уязвимостям безопасности информации, в том числе зарубежными информационными ресурсами;

2.3.3. разработки необходимых документов в интересах организации работ по защите информации от НСД;

2.3.4. выявления угроз безопасности информации в автоматизированных (информационных) системах;

2.3.5. участия в разработке организационных и технических мероприятий по защите объектов информатизации от НСД к информации, контроля их выполнения;

2.3.6. установки, применения и настройки современных средств защиты информации от НСД;

проведения работ по контролю защищенности информации от НСД.

**3.Категория слушателей** (возможно заполнение не всех полей)

* 1. Среднее профессиональное или высшее образование в области математических или естественных наук, инженерного дела, технологий и технических наук, подтвержденное документом об образовании
  2. Техник, бакалавр или специалист
  3. рекомендуется
  4. Не предусмотрено

**4.Учебный план программы «Способы и средства защиты информации от несанкционированного доступа в условиях цифровой трансформации»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1. | Модуль 1 | 30 | 6 | 8 | 16 |
| 2. | Модуль 2 | 40 | 6 | 16 | 18 |
| **Итоговая аттестация** | |  | **Указывается вид (экзамен, зачёт, реферат и т.д.)** | | |
| 3. | | 2 | зачет | | |

**5.Календарный план-график реализации образовательной** программы

(дата начала обучения – дата завершения обучения) в текущем календарном году, указания на периодичность набора групп (не менее 1 группы в месяц)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| **1** | Модуль 1. Организация работ по технической защите информации | 30 | 02.11- 06.11.2020г. |
| **2** | Модуль 2. Защита информации от несанкционированного доступа | 40 | 09.11-14.11.2020г. |
| **Всего:** | | 72 | 02.11-13.11.2020г. |

**6.Учебно-тематический план программы «**  Способы и средства защиты информации от несанкционированного доступа в условиях цифровой трансформации **»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Организация работ по технической защите информации | 30 | 6 | 8 | 16 |  |
| 1.1 | Цели и задачи ТЗИ, угрозы безопасности информации, связанные с НСД | 14 | 2 | 4 | 8 |  |
| 1.2 | Формирование требований по защите информации и создание системы защиты информации от НСД | 16 | 4 | 4 | 8 |  |
| 2 | Защита информации от несанкционированного доступа | 40 | 6 | 16 | 18 |  |
| 2.1 | Меры и средства защиты информации от НСД | 26 | 2 | 12 | 12 |  |
| 2.2 | Основные задачи контроля состояния технической защиты информации от несанкционированного доступа | 14 | 4 | 4 | 6 |  |

**7. Учебная (рабочая) программа повышения квалификации «** Способы и средства защиты информации от несанкционированного доступа в условиях цифровой трансформации  **»**

**Модуль 1.** Организация работ по технической защите информации **(** 30 **час.)**

**Тема 1.1** Цели и задачи ТЗИ, угрозы безопасности информации, связанные с НСД **(** 14 **час)**

1.1. Цели и задачи ТЗИ, угрозы безопасности информации, связанные с НСД.

Основные термины и определения в области ТЗИ. Государственная система ПД ИТР и ТЗИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации. Цели и задачи ТЗИ.

Объекты защиты информации. Защищаемые информация и информационные ресурсы. Объекты информатизации, их классификация и характеристика.

Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций.

Понятие, классификация и технологии построения информационных систем. Информационные системы как объекты защиты от НСД. Стандартная модель взаимодействия открытых систем и протоколы межсетевого взаимодействия.

Понятие и классификация угроз безопасности информации, связанных с НСД. Источники угроз безопасности информации от НСД.

Модели угроз безопасности информации от НСД.

Методы выявления и анализа угроз безопасности информации. Уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

Банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE. Общая система оценки уязвимостей (стандарт CVSS).

**Тема 1.2** Формирование требований по защите информации и создание системы защиты информации от НСД ( 16 час)

Правовые основы защиты информации. Система документов в области ТЗИ. Нормативные правовые акты. Нормативные правовые акты ФСТЭК России. Методические документы. Технические документы (документация). Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Общие вопросы организации лицензирования деятельности в области ТЗИ, сертификации средств защиты информации, аттестации объектов информатизации по требованиям безопасности информации. Ответственность за правонарушения в области защиты информации.

Формирование требований по защите информации от НСД, содержащейся в информационной системе (на объекте информатизации).

Требования по защите информации от НСД.

Требования международных стандартов по защите информации от НСД.

Создание и функционирование системы защиты информации как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий.

Стадии этапов создания системы защиты информации.

Комплекс работ по созданию системы защиты информации (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации).

**Модуль 2.** Защита информации от несанкционированного доступа **(**40 **час.)**

**Тема 2.1.** Меры и средства защиты информации от НСД (26 час.)

Комплекс мероприятий по ТЗИ от НСД.

Особенности защиты информации от НСД при использовании современных информационных технологий (мобильных, беспроводных, грид, суперкомпьютерных, виртуализации, облачных, больших данных и др.)

Обеспечение защиты информации от НСД в ходе эксплуатации аттестованной информационной системы.

Обеспечение защиты информации от НСД при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Общая характеристика и классификация мер и средств защиты информации от НСД.

Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД. Особенности создания системы защиты информации от НСД как обеспечивающей подсистемы автоматизированной (информационной) системы. Системные и документальные части системы защиты информации от НСД.

Средства защиты информации от НСД. Межсетевые экраны, требования к ним и способы применения. Системы обнаружения вторжений, требования к ним и способы применения. Средства антивирусной защиты, требования к ним и способы применения. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа. Средства регистрации и учета. Средства (механизмы) обеспечения целостности информации. Криптографические средства защиты информации. Перспективные технологии биометрической аутентификации. DLP-системы, их возможности и перспективы применения.

Установка и настройка средств защиты информации от НСД.

Общий порядок разработки и производства средств защиты информации от НСД.

Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности.

Тема 2.2. Основные задачи контроля состояния технической защиты информации от несанкционированного доступа (14 час.)

Классификация видов контроля состояния ТЗИ от НСД.

Система документов по контролю состояния ТЗИ от НСД.

Вопросы, подлежащие проверке при контроле состояния ТЗИ от НСД в организации.

Организационный и технический контроль состояния ТЗИ от НСД.

Классификация методов контроля защищенности информации от НСД и их характеристики. Сканеры безопасности и их характеристики. Средства анализа программных кодов и их характеристика. Средства антивирусной защиты и их характеристика.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Программы и методы аттестационных испытаний. Заключение по результатам аттестации объектов информатизации. Аттестат соответствия объекта информатизации.

Порядок проведения работ по сертификации продукции, используемой в целях защиты информации от НСД.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| **1.** | 1.1. | Разработка концепции обеспечения информационной безопасности предприятия | Приобретение навыков работы с организационно-распорядительной документацией предприятия в области информационной безопасности предприятия. |
| 2. | 1.2. | Разработка плановых документов предприятия по защите информации от НСД | Приобретение навыков работы с организационно-распорядительной документацией предприятия в области информационной безопасности предприятия. |
| 3. | 2.1. | ROSA «Кобальт» Операционная система для обработки персональных данных и конфиденциальной информации | Приобретение навыков установки, настройки, эксплуатации. |
| 4. | 2.1. | СЗИ от НСД Dallas Lock 8.0-K Защита от НСД в информационных системах, обрабатывающих конфиденциальную информацию | Приобретение навыков установки, настройки, эксплуатации. |
| 5. | 2.1. | СЗИ от НСД Dallas Lock 8.0-C Защита от НСД в информационные системы, обрабатывающие конфиденциальную информацию и информацию, содержащую сведения, составляющие государственную тайну | Приобретение навыков установки, настройки, эксплуатации. |
| 6. | 2.1. | Средство защиты информации Secret Net Studio | Приобретение навыков установки, настройки, эксплуатации. |
| 7. | 2.1. | Средство защиты информации Secret Net Studio – C | Приобретение навыков установки, настройки, эксплуатации. |
| 8. | 2.1. | СЗИ от НСД Страж NT 4.0 | Приобретение навыков установки, настройки, эксплуатации. |
| 9. | 2.2. | Операционная система специального назначения  Astra Linux Special Edition | Приобретение навыков установки, настройки, эксплуатации. |
| 10. | 2.2. | АЛЬТ 8 СП Операционная система для обработки, хранения и передачи информации в защищенной программной среде | Приобретение навыков установки, настройки, эксплуатации. |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| **1.1** | 1. Дать определение информационной безопасности.  2. Дать определение конфиденциальности информации.  3. Дать определение целостности информации.  4. Дать определение доступности информации.  5. Дать определение аутентичности.  6. Дать определение угрозы информационной безопасности.  7. Дать определение атаки.  8. Дать определение злоумышленника.  9. Дать определение информации.  10. Дать определение информационной системы.  11. Дать определение обладателя информации.  12. Дать определение конфиденциальности информации.  13. Дать определение защиты информации.  14. Дать определение нарушителя безопасности  15. Дать определение контролируемой зоны.  16. Дать определение санкционированного доступа к информации  17. Дать определение несанкционированного доступа к информации.  18. Дать определение защиты от несанкционированного доступа.  19. Что является объектом защиты информации.  20. Какие задачи решает система защиты информации предприятия. | Промежуточное тестирование осуществляется на каждом практическом занятии | 1. Дать определение угрозы информационной безопасности.  2. Дать определение атаки.  3. Дать определение злоумышленника.  4. Дать определение информационной системы.  5. Дать определение обладателя информации.  6. Дать определение конфиденциальности информации.  7. Дать определение защиты информации.  8. Дать определение нарушителя безопасности  9. Дать определение контролируемой зоны.  10. Дать определение санкционированного доступа к информации  11. Дать определение несанкционированного доступа к информации.  12. Дать определение защиты от несанкционированного доступа.  13. Что является объектом защиты информации.  14. Что такое Astra Linux?  15. Какую информацию Astra Linux позволяет обрабатывать?  16. Что включает в себя Asta Linux?  17. Какие релизы Astra Linux существуют? Выберите правильные ответы.  18. Можно ли использовать Astra Linux со средствами доверенной загрузки?  19. Какие действия необходимо выполнить на компьютере, который будет использоваться в качестве сервера безопасности Secret Net Studio?  20. Из каких программных пакетов состоит Secret Net Studio?  21. Что произойдёт в случае отсутствия обновления 8.5.5329.40 после установки программы управления Secret Net Studio?  22. В каких из следующих вариантов может выполняться установка сервера безопасности Secret Net Studio?  23. Что произойдёт, если изменить имя компьютера при установленном на нём компонента «Сервер безопасности» Secret Net Studio?  24. Поддерживает ли сервер безопасности Secret Net Studio режим аутентификации Windows при работе с сервером СУБД?  25. Какие учётные данные необходимо вводить для соединения с БД?  26. После установки программы управления Secret Net Studio нужно ли устанавливать пакет обновлений 8.5.5329.40?  27. На основе какой операционной системы создана Альт 8 СП?  28. Что используется в качестве загрузчика в Альт 8?  29. В каком виде поставляется Альт 8 СП?  30. С сервером в режиме ручного изменения времени в Альт 8 СП доступна активация функции синхронизации?  31. Для каких целей профиль установки сервера “Сервер Samba-DC” предлагает группу пакетов?  32. Что доступно при настройке сетевых параметров в Альт 8 СП?  33. Какой из перечисленных TCP/IP портов должен быть открыт на межсетевом экране для успешного обмена данными между Сервером безопасности и Клиентом Dallas Lock?  34. Какое программное обеспечение необходимо для предоставления возможности удаленного подключения к Серверу безопасности Dallas Lock с рабочего места администратора безопасности?  35. Какой компонент Dallas Lock необходимо установить на локальный компьютер перед установкой любого другого компонента Dallas Lock?  36. Какой компонент Dallas Lock позволяет осуществлять централизованное управление политиками и управлять доменами безопасности в организации?  37. К какой группе обязательно должен относится пользователь, осуществляющий установку Клиент Dallas Lock?  38. Какая команда позволяет запустить редактор оснасток Клиент Dallas Lock, в котором можно добавить консоль управления пользователями и группами?  39. Какую роль автоматически получает пользователь, установивший Dallas Lock на локальном компьютере, в терминологии Dallas Lock?  40. Какое действия обязательно должно быть выполнено сразу после установки клиента Dallas Lock?  41. Какой из перечисленных способов размещения сервера баз данных Клиент Dallas Lock является наиболее рекомендуемым?  42. Что из себя представляет СЗИ Dallas Lock Linux?  43. Какие из перечисленных файловых систем поддерживает Dallas Lock Linux?  44. Соответствует ли Dallas Lock Linux требованиям ФСТЭК России по защищенности СВТ от НСД?  45. Соответствует ли Dallas Lock Linux требованиям ФСТЭК России по уровню контроля отсутствия НДВ?  46. Какие аппаратные идентификаторы НЕ поддерживает Dallas Lock Linux?  47. Какие из перечисленных функций НЕ поддерживает Dallas Lock Linux?  48. Какие из перечисленных операционных систем официально НЕ поддерживает Dallas Lock Linux?  49. Rosa «Кобальт» является дистрибутивом какой операционной системы?  50. Rosa «Кобальт» разработана для каких систем?  51. Какие сертификаты имеет Rosa «Кобальт»?  52. Для каких структур подходит Rosa «Кобальт»?  53. Какие функции реализует Rosa «Кобальт»?  54. СЗИ Страж NT 4.0 применяется в автоматизированных системах до класса защищенности ### включительно?  55. СЗИ Страж NT 4.0 применяется в государственных информационных системах до ### класса защищенности включительно?  56. СЗИ Страж NT 4.0 применяется в информационных системах персональных данных до ### уровня защищенности включительно?  57. Какие режимы запуска существуют в СЗИ Страж NT 4.0?  58. Какой режим установлен в СЗИ Страж NT 4.0 в качестве режима запуска по умолчанию?  59. Какие значения меток конфиденциальности В СЗИ Страж NT 4.0 используются по умолчанию?  60. Какие процедуры выполняются при настройке разграничения доступа пользователей к устройствам СЗИ Secret Net –C?  61. В списке устройств групповой политики СЗИ Secret Net –C можно добавлять сведения о конкретных устройствах?  62. Что содержит PID СЗИ Secret Net –C?  63. В каком случае процедура расчета эталонов СЗИ Secret Net –C выполняется автоматически?  64. Для чего предназначен механизм замкнутой программной среды СЗИ Secret Net –C?  65. Что не относится к функциям СЗИ Secret Net –C?  66. Можно ли отредактировать список учетных записей при настройке прав доступа к устройству СЗИ Secret Net –C? |

**8.2.**  При входном тестировании претендент на обучение должен ответить не менее чем на 50% сформулированных вопросов **.**

**8.3.**  Пример задания на практическую работу:

выполнить запрос демонстрационной версии СЗИ Dallas Lock 8.0-C на сайте производителя СЗИ;

выполнить развертывание доменной инфраструктуры Active Directory для последующей интеграции с Dallas Lock

выполнить развертывание компонентов Dallas Lock, необходимых для функционирования Сервера безопасности Dallas Lock;

выполнить развертывание компонентов Dallas Lock, необходимых для функционирования рабочего места администратора безопасности;

выполнить развертывание компонентов Dallas Lock, необходимых для функционирование рабочего места пользователя.

Список рекомендованных источников для выполнения задания и закрепления изученного материала

1. Чипига, А. Ф. Информационная безопасность автоматизированных систем: учеб. пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности / А. Ф. Чипига. – М.: Гелиос АРВ, 2010. – 336 с., ил.

2. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – М.: ДМК-Пресс, 2008. – 544 с.

3. Мельников В. П. Информационная безопасность и защита информации: учебное пособие для студ. высш. учеб. заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под. ред. С. А. Клейменова. — 3-е изд., стер. — М.: Издательский центр «Академия», 2008. — 336 с.

4. Документация СЗИ НСД Dallas Lock 8.0-С [Электронный ресурс]. Режим доступа: https://dallaslock.ru/products/szi-nsd-dallas-lock/szi-ot-nsd-dallas-lock-8-0-s/ (дата обращения: 12.10.2020) **.**

**8.4.**  Вопросы для тестирования после выполнения практического занятия для приведенного примера (Разработаны для всех практических занятий)

Какая роль Windows Server позволяет осуществить развертывание домена Active Directory:

- Службы сертификации Active Directory

- Службы федерации Active Directory

+ Доменные службы Active Directory

- Службы развертывания Windows

Какая функция должна быть активирована на контроллере домена Active Directory для функционирования Dallas Lock:

- DHCP сервер

+ DNS сервер

- Веб-сервер

- Файловый сервер

К какой группе обязательно должен относится пользователь, осуществляющий установку Клиент Dallas Lock, с использованием домена Active Directory:

+ Администраторы домена

- Гостевая группа

- Сетевые администраторы

- Бухгалтерия

Какой из перечисленных TCP/IP портов должен быть открыт на межсетевом экране для успешного обмена данными между Сервером безопасности и Клиентом Dallas Lock:

- 5436

- 80

+ 17493

- 443

Какое программное обеспечение необходимо для предоставления возможности удаленного подключения к Серверу безопасности Dallas Lock с рабочего места администратора безопасности:

- Сервер конфигураций Dallas Lock

+ Консоль сервера безопасности

- Сервер лицензий

- Putty

Какой компонент Dallas Lock необходимо установить на локальный компьютер перед установкой любого другого компонента Dallas Lock:

+ Клиент Dallas Lock

- Сервер лицензий

- Сервер безопасности

- Консоль сервера безопасности

Какой компонент Dallas Lock позволяет осуществлять централизованное управление политиками и управлять доменами безопасности в организации:

- Сервер лицензий

- Клиент Dallas Lock

+ Сервер безопасности

- Консоль сервера безопасности

Какую роль автоматически получает пользователь, установивший Dallas Lock на локальном компьютере, в терминологии Dallas Lock:

- Администратор безопасности

- Администратор Dallas Lock

+ Суперадминистратор

- Гостевой пользователь

Какое действия обязательно должно быть выполнено сразу после установки клиента Dallas Lock:

+ Перезагрузка компьютера

- Выход пользователя из системы

- Обновление операционной системы

- Отключение от локальной сети

Какой из перечисленных способов размещения сервера баз данных Клиент Dallas Lock является наиболее рекомендуемым:

- Размещение сервера баз данных на виртуальной машине, запущенной на сервере безопасности

+ Размещение сервера баз данных на выделенном физическом сервере

- Размещение сервера баз данных на виртуальной машине, запущенной в центре обработки данных облачного провайдера

- Размещение сервера баз данных непосредственно на сервере безопасности **.**

**8.5.**  Успешно окончившим курс обучения считается слушатель, правильно ответивший не менее чем на 50% вопросов итогового тестирования **.**

**9.Организационно-педагогические условия реализации программы**

**9.1. Кадровое обеспечение программы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Фамилия, имя, отчество (при наличии)** | **Место основной работы и должность, ученая степень и ученое звание (при наличии)** | **Ссылки на веб-страницы с портфолио (при наличии)** | **Фото в формате jpeg** | **Отметка о полученном согласии на обработку персональных данных** |
| **1** | Чипига Александр Федорович | СКФУ, заведующий кафедрой информационной безопасности автоматизированных систем, кандидат технических наук, профессор | <https://www.ncfu.ru/for-employee/list-of-employees/employee/23700685-1e28-11e9-bd69-0050568c7ce8/> |  | согласен |

**9.2.Учебно-методическое обеспечение и информационное сопровождение**

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Практико-ориентированное обучение и деятельностный подход. Онлайн-обучение, метод кейсов.  Онлайн-лекции, видео-лекции  Практические занятия, практико-ориентированные контрольные задания. | Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. – М.: Форум, 2012. – 352 с.  Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства: Учебное пособие. – М.: ДМК Пресс, 2008. – 544 с.  Шаньгин В.Ф. Комплексная защита корпоративной информации: Учебное пособие. – М.: МИЭТ, 2009. – 404 с.  Новиков В.К. Организационное и правовое обеспечение информационной безопасности: Учебное пособие. В 2-х ч. Ч. 1. Правовое обеспечение информационной безопасности. – М.: МИЭТ, 2013. – 184 с.  Новиков В.К. Организационное и правовое обеспечение информационной безопасности: Учебное пособие. В 2-х ч. Ч. 2. Правовое обеспечение информационной безопасности. – М.: МИЭТ, 2013. – 172 с.; |
|  |  |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| Онлайн-обучение.  Онлайн-лекции, видео-лекции.  Практические занятия, практико-ориентированные контрольные задания. | <https://astralinux.ru/products/astra-linux-special-edition/>  <http://altsp.su/>  <https://www.rosalinux.ru/products/rosa-cobalt/>  <https://www.dallaslock.ru/products/szi-nsd-dallas-lock/szi-ot-nsd-dallas-lock-8-0-k/>  <https://www.dallaslock.ru/products/szi-nsd-dallas-lock/szi-ot-nsd-dallas-lock-8-0-s/>  <https://www.dallaslock.ru/products/szi-nsd-dallas-lock-linux/>  <https://www.securitycode.ru/products/secret-net-studio/>  <https://www.securitycode.ru/products/secret-net-studio/>  <https://www.securitycode.ru/products/szi_secret_net/>  <https://www.securitycode.ru/products/szi_secret_net/>  <https://guardnt.ru/gnt_40.html/> |
|  |  |

**9.3.Материально-технические условия реализации программы**

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Онлайн-лекция | Персональный компьютер или ноутбук  Офисные приложения: MS Excel, MS PowerPoint (версия 10-16)  Возможность выхода в сеть Интернет  LMS Moodle  Подключение к вебинарной площадке BigBlueButton |
| Практическое занятие | Персональный компьютер или ноутбук  Виртуальная машина  Возможность выхода в сеть Интернет |
| Контрольное занятие (тестирование) | Персональный компьютер или ноутбук  Возможность выхода в сеть Интернет |

**III.Паспорт компетенций (Приложение 2)**

Описание перечня профессиональных компетенций, качественное изменение которых осуществляется в результате обучения.

Планируемые результаты обучения должны быть определены в виде знаний, умений, навыков и (или) опыта деятельности, характеризующих формирование/развитие компетенции(-й) в области цифровой экономики и представлены в виде Паспорта компетенций в машиночитаемом текстовом формате. Структура паспорта представлена в приложении.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | способность формировать требования по технической защите информации (ТЗИ) от несанкционированного доступа (НСД) на объектах информатизации (формировать требования к системе защиты информации объекта информатизации) | |  | |
| 2. | Указание типа компетенции |  |  | |
|  |  | |
| профессиональная | профессиональная | |
|  |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Слушатель должен:  а) знать:  нормативные правовые акты Российской Федерации, нормативные и методические документы в области ТЗИ (защиты информации от НСД);  основные понятия в области ТЗИ;  порядок проведения работ по сертификации средств защиты информации по требованиям безопасности информации.  б) уметь:  анализировать угрозы безопасности информации;  определять требования к средствам защиты информации от НСД.  в) владеть навыками:  работы с нормативными правовыми актами, методическими документами, национальными и международными стандартами в области ТЗИ;  работы с базами данных, содержащих информацию по угрозам и уязвимостям безопасности информации, в том числе зарубежными информационными ресурсами;  выявления угроз безопасности информации в автоматизированных (информационных) системах. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | |  |  |
|  | |  |  |
|  | |  |  |
|  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | а) знает:  нормативные правовые акты Российской Федерации, нормативные и методические документы в области ТЗИ (защиты информации от НСД);  основные понятия в области ТЗИ;  порядок проведения работ по сертификации средств защиты информации по требованиям безопасности информации.  б) умеет:  анализировать угрозы безопасности информации;  определять требования к средствам защиты информации от НСД.  в) владеет навыками:  работы с нормативными правовыми актами, методическими документами, национальными и международными стандартами в области ТЗИ;  работы с базами данных, содержащих информацию по угрозам и уязвимостям безопасности информации, в том числе зарубежными информационными ресурсами;  выявления угроз безопасности информации в автоматизированных (информационных) системах. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Компетенции цифровой грамотности | |
| 6. | Средства и технологии оценки | | Тесты, задания для практического выполнения | |

ПАСПОРТ КОМПЕТЕНЦИИ

(Способы и средства защиты информации от несанкционированного доступа в условиях цифровой трансформации)

(Северо-Кавказский федеральный университет)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | способность внедрять способы и средства ТЗИ от НСД на объектах информатизации (внедрять системы защиты информации объекта информатизации) | |  | |
| 2. | Указание типа компетенции |  |  | |
|  |  | |
| профессиональная | профессиональная | |
|  |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Освоившие программу должны:  а) знать:  систему организации защиты информации, действующей в органе государственной власти, организации;  основы методологии и методики проведения ТЗИ от НСД в органе государственной власти, организации;  б) уметь:  проводить обоснование выбора современных способов и средств защиты информации от НСД;  проводить мероприятия по защите информации от НСД;  в) владеть навыками:  участия в разработке организационных и технических мероприятий по защите объектов информатизации от НСД к информации, контроля их выполнения. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | |  |  |
|  | |  |  |
|  | |  |  |
|  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | а) знает:  систему организации защиты информации, действующей в органе государственной власти, организации;  основы методологии и методики проведения ТЗИ от НСД в органе государственной власти, организации;  процедуры выявления угроз безопасности информации на объектах информатизации, организации.  б) умеет:  проводить обоснование выбора современных способов и средств защиты информации от НСД;  проводить мероприятия по защите информации от НСД.  в) владеет навыками:  участия в разработке организационных и технических мероприятий по защите объектов информатизации от НСД к информации, контроля их выполнения. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Компетенции цифровой грамотности | |
| 6. | Средства и технологии оценки | | Тесты, задания для практического выполнения | |
| 1. | способность обеспечивать ТЗИ от НСД в ходе эксплуатации объектов информатизации | |  | |
| 2. | Указание типа компетенции |  |  | |
|  |  | |
| профессиональная | профессиональная | |
|  |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Освоившие программу должны:  а) знать:  способы и средства защиты информации от НСД;  требования к средствам защиты информации от НСД;  цели, задачи, основные принципы организации, методы и средства ведения контроля состояния защищенности информации в органе государственной власти, организации;  порядок оформления технической документации по защите информации.  б) уметь:  устанавливать, применять и настраивать средства защиты информации от НСД;  разрабатывать проекты нормативных и методических документов по защите объектов информатизации от НСД к информации;  осуществлять проверку выполнения требований нормативных документов по защите информации от НСД;  осуществлять контроль защищенности информации от НСД.  в) владеть навыками:  разработки необходимых документов в интересах организации работ по защите информации от НСД;  установки, применения и настройки современных средств защиты информации от НСД;  проведения работ по контролю защищенности информации от НСД. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | |  |  |
|  | |  |  |
|  | |  |  |
|  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | а) знает:  способы и средства защиты информации от НСД;  требования к средствам защиты информации от НСД;  цели, задачи, основные принципы организации, методы и средства ведения контроля состояния защищенности информации в органе государственной власти, организации;  порядок оформления технической документации по защите информации.  б) умеет:  разрабатывать проекты нормативных и методических документов по защите объектов информатизации от НСД к информации;  осуществлять проверку выполнения требований нормативных документов по защите информации от НСД;  осуществлять контроль защищенности информации от НСД.  в) владеет навыками:  разработки необходимых документов в интересах организации работ по защите информации от НСД;  установки, применения и настройки современных средств защиты информации от НСД;  проведения работ по контролю защищенности информации от НСД.  . |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Компетенции цифровой грамотности | |
| 6. | Средства и технологии оценки | | Тесты, задания для практического выполнения | |

**VI.Иная информация о качестве и востребованности образовательной программы** (результаты профессионально-общественной аккредитации образовательной программы, включение в системы рейтингования, призовые места по результатам проведения конкурсов образовательных программ и др.) (при наличии)

**V.Рекомендаций к программе от работодателей**: наличие не менее двух писем и/или подтверждения на цифровой платформе Государственной системы предоставления ПЦС от работодателей о рекомендации образовательной программы для реализации в рамках Государственной системы предоставления ПЦС на формирование у трудоспособного населения компетенций цифровой экономики с указанием востребованности результатов освоения программы в сфере деятельности соответствующих компаний и готовности к рассмотрению заявок наиболее успешно освоивших образовательную программу граждан на прохождение стажировки и (или) собеседования на предмет трудоустройства путем проставления отметки в профиле программы

 