Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Южно-Российский институт управления

ЮРИУ РАНХиГС
ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0E9405C017SB8A6CEC7B031C2FEE708F
Владелец: Рудой Василий Владимирович
Действителен: с 15.07.2025 до 08.10.2026

Директор
Южно-Российского института управления – филиала РАНХиГС

_____ В.В. Рудой
«26» февраля 2026 г.

УТВЕРЖДЕНА
ученым советом ЮРИУ РАНХиГС (*филиала*)
Протокол от «26» февраля 2026 г. № 53

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации

Специалист по защите информации в организациях бюджетной сферы

г. Ростов-на-Дону, 2026 г.

Разработчики

Заместитель директора ЮРИУ РАНХиГС _____ (подпись) А.В. Баранов

Директор инновационно-технологического центра ЮРИУ РАНХиГС _____ (подпись) В.М. Ганеева

Директор программы центра дополнительного образования ЮРИУ РАНХиГС _____ (подпись) А.С. Санин

Доцент кафедры менеджмента ЮРИУ РАНХиГС _____ (подпись) В.Х. Тирацуян

Руководитель программы

Заместитель директора ЮРИУ РАНХиГС _____ (подпись) А.В. Баранов

Руководитель структурного подразделения

Директор инновационно-технологического центра ЮРИУ РАНХиГС _____ (подпись) В.М. Ганеева

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ 4
   - 1.1. Цель реализации 4
   - 1.2. Нормативно-правовая база 4
   - 1.3. Планируемые результаты обучения 5
   - 1.4. Категория слушателей 10
   - 1.5. Форма и технологии обучения 10
   - 1.6. Период обучения, срок освоения и режим занятий 10
   - 1.7. Документ о квалификации 10
2. СОДЕРЖАНИЕ ПРОГРАММЫ 11
   - 2.1. Календарный учебный план 11
   - 2.2. Учебный план 12
   - 2.3. Содержание программы дисциплин (модулей) 17
3. ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ 17
   - 3.1. Материально-техническое и программное обеспечение реализации программы 25
   - 3.2. Учебно-методическое и информационное обеспечение программы 29
4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ 35
5. ИНДИКАТОР СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ 48

1. Общая характеристика программы

1.1. Цель реализации

Цель программы: Формирование комплексных знаний и практических навыков для выполнения трудовых функций специалиста по защите информации в бюджетной сфере, включая внедрение, администрирование и мониторинг систем информационной безопасности.

Задачи программы:

1. Сформировать системное понимание архитектуры современных телекоммуникационных сетей (фиксированных и мобильных) и протоколов передачи данных.
2. Изучить нормативно-правовую базу в области защиты информации (ФЗ-152, ФСТЭК, ФСБ, регуляторы связи).
3. Освоить принципы, методы и средства криптографической защиты информации и управления ключами.
4. Сформировать навыки анализа угроз и уязвимостей в телеком-системах, проведения аудита защищенности.
5. Отработать практические приемы обнаружения, анализа и реагирования на инциденты информационной безопасности.

1.2. Нормативно-правовая база

Дополнительная профессиональная программа повышения квалификации разработана на основе следующих нормативных документов:

1. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (ред. от 04.08.2023).
2. Постановление Правительства РФ от 12.05.2012 г. № 473 «Об утверждении устава федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (ред. от 29.05.2023)
3. Приказ Министерства образования и науки Российской Федерации от 01.07.2013г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (ред. от 15.11.2013).
4. Приказ Министерства образования и науки Российской Федерации от 12.09.2013г. № 1061 «Об утверждении перечней и специальностей подготовки высшего образования» (ред. от 13.12.2021).
5. Методические рекомендации Министерства образования и науки Российской Федерации от 10.04.2014г. № 06-381 «Методические рекомендации по использованию электронного обучения, дистанционных образовательных технологий при реализации дополнительных профессиональных образовательных программ».
6. Методические рекомендации Министерства образования и науки Российской Федерации от 22.01.2015г. № ДЛ-1/05вн «Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов».
7. Приказ Министерства труда и социальной защиты РФ от 14 сентября 2022 г. №536н «Об утверждении профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях».
8. Приказ Министерства труда и социальной защиты РФ от 31 октября 2018 г. № 682н «Об утверждении профессионального стандарта «Консультант в области развития цифровой грамотности населения (цифровой куратор)».
9. Приказ Министерства труда и социальной защиты РФ от 17 апреля 2018 г. № 248н «Об утверждении профессионального стандарта «Специалист по процессному управлению».

10. Приказ ректора РАНХиГС «Об утверждении образовательного стандарта Академии по направлению подготовки 38.03.04 «Государственное и муниципальное» от 29.03.2021 г. № 01-3023

11. Приказ РАНХиГС «Об утверждении Положения о применении в Академии электронного обучения, дистанционных образовательных технологий при реализации программ» от 22.09.2017г. № 01-6230.

12. Приказ РАНХиГС «Об утверждении локальных нормативных актов РАНХиГС по дополнительному профессиональному образованию» от 19.04.2019г. № 02-461.

13. Приказ РАНХиГС «Об утверждении положения о порядке разработки и утверждения в РАНХиГС дополнительных профессиональных программ – программ профессиональной переподготовки, программ повышения квалификации» от 13.08.2021г. № 02-835 (с изменениями и дополнениями от 30.06.2023г.)

14. ОКВЭД-2 Общероссийский классификатор видов экономической деятельности ОК 029-2014 (КДЕС Ред. 2) по состоянию на 2021 год (в ред. Изменения 01/2015 ОКВЭД2, утв. Приказом Росстандарта от 26.05.2015 № 423-ст, 02/2015 ОКВЭД 2, утв. Приказом Росстандарта от 17.08.2015 № 1165-ст)

15. Единый квалификационный справочник должностей руководителей, специалистов и других служащих, Раздел I, Общеотраслевые квалификационные характеристики должностей работников, занятых на предприятиях, в учреждениях и организациях, утвержденный Постановлением Минтруда РФ от 21.08.1998 № 37 (ред. от 27.03.2018).

При формировании образовательной программы учтены следующие документы:

1. Методические рекомендации по установлению квалификационных требований для замещения должностей муниципальной службы и организации оценки на соответствие указанным требованиям https://mintrud.gov.ru/ministry/programms/municipal_service/0;

2. Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов (утв. Минобрнауки России 22.01.2015 № ДЛ-1/05вн);

3. Методические рекомендации-разъяснения по разработке дополнительных профессиональных программ на основе профессиональных стандартов (утв. Минобрнауки России 22.04.2015 № ВК-1032/06);

4. Методические рекомендации по использованию электронного обучения, дистанционных образовательных технологий при реализации дополнительных профессиональных образовательных программ, направленные письмом Министерства образования и науки Российской Федерации от 10.04.2014 № 06-381.

1.3. Планируемые результаты обучения

Указываются виды деятельности и перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения и (или) получение новой компетенции необходимой для профессиональной деятельности, а также знания, умения и практический опыт, приобретаемый в результате освоения программы (таблица 1).

Планируемые результаты обучения

Виды деятельности	Общепрофессиональные, профессионально-специализированные компетенции или трудовые функции (ОПК, ПСК, ПЛК) *(формируются и (или) совершенствуются)*	Знания	Умения	Практический опыт
Выполнение комплекса мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НД и компьютерных атак	ПСК – 1.[1] Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД	Знать: - нормативные правовые акты в области связи, информатизации и защиты информации; - нормативные требования к составу и содержанию эксплуатационной документации СССЭ, а также средств и систем защиты СССЭ от НД; - номенклатура, функциональное назначение и основные характеристики средств и систем защиты СССЭ от НД; - номенклатура, функциональное назначение и основные характеристики СССЭ	Уметь: - проводить проверку комплектности СССЭ, средств и систем защиты СССЭ от НД; -проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НД	Владеть навыками: - первичная настройка и проверка функционирования СССЭ; - монтаж программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД; - первичная настройка и проверка функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД
	ПСК – 2.[2] Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НД, средств для поиска признаков компьютерных атак в сетях электросвязи	Знать: -нормативные правовые акты в области связи, информатизации и защиты информации, обеспечения безопасности критической информационной инфраструктуры; - организационные меры по защите информации; -типы, основные характеристики средств измерений и контроля процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи; - последовательность действий в целях изменения настроек СССЭ, а также средств и систем защиты СССЭ от НД, средств для поиска признаков	Уметь: -проводить текущий контроль показателей и процесса функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи, предусмотренный регламентом их эксплуатации; - выполнять предусмотренные в технической документации работы по изменению настроек СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от	Владеть навыками: - текущий, в том числе автоматизированный, контроль функционирования с установленными показателями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи; - внесение изменений в настройки СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях

[1] Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 536н (трудовая функция А/01.5)

[2] Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 536н (трудовая функция А/02.5)

		компьютерных атак в сетях электросвязи без прерывания процесса их функционирования	НД, средств для поиска признаков компьютерных атак в сетях электросвязи	электросвязи без прерывания процесса их функционирования; - восстановление процесса функционирования после сбоев и отказов СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи
Обеспечение защиты от НД и компьютерных атак сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации	ПСК – 3.[3] Мониторинг функционирования СССЭ, защищенности от НД и компьютерных атак сооружений и СССЭ	Знать: -нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации по вопросам обеспечения информационной безопасности СССЭ; -возможные источники и технические каналы утечки информации; -методы контроля функционирования СССЭ, их защищенности от НД и компьютерных атак	Уметь: -использовать установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации формы документов, сопровождающих жизненный цикл объекта критической информационной инфраструктуры; -использовать средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты СССЭ от НД и компьютерных атак; - проводить контроль функционирования СССЭ, их защищенности от НД и компьютерных атак; -определять технические характеристики СССЭ, их защищенности от НД и компьютерных атак	Владеть навыками: - анализ функциональности СССЭ, защищенности от НД сооружений и СССЭ; - составление отчетов по результатам проверок, в том числе выявление инцидентов, которые могут привести к сбоям или нарушению функционирования или возникновению угроз безопасности информации, циркулирующей в СССЭ; -доведение сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости до федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

[3] Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 536н (трудовая функция B/01.6)

Консультирование граждан в области развития цифровой грамотности	ПСК – 4[4]. Ознакомительное индивидуальное консультирование граждан в области информационно-коммуникационных технологий	Знать: - правила деловой переписки и письменного этикета; -правила делового общения и речевого этикета; - сведения об организациях и специалистах, содействующих в коммуникации с людьми с ограниченными возможностями; -требования к оформлению документации; - принципы построения и функционирования баз данных и особенности работы с ними; - основные функции операционных и файловых систем; -основные программы, входящие в пакет типовых приложений в составе операционной системы; -методы обработки текстовой, численной и графической информации	Уметь: - организовывать консультирование граждан с ограниченными возможностями с привлечением специалистов; - оформлять заявки на предоставление консультационных услуг в соответствии с установленными формами; - обрабатывать персональные данные с соблюдением требований, установленных законодательством Российской Федерации; - оказывать консультативную помощь, связанную с оперированием персональными данными самими пользователями (и их защитой) при работе с интернет-сервисами; - применять различные методы поиска информации в информационно-телекоммуникационной сети «Интернет»	Владеть навыками: - ведение непосредственного приема обращений граждан; - электронная коммуникация по обращениям граждан; -поиск и обработка информации, необходимой для проведения консультаций в соответствии с рабочим заданием; - визуальное и дистанционное размещение информации и проведение консультаций; - ведение базы данных граждан, обратившихся за консультацией; - ответы на вопросы граждан, связанные с цифровой тематикой; - консультировать граждан под руководством специалиста, проявлять самостоятельность при решении типовых задач; -вести диалог, учитывая возрастные и индивидуальные особенности собеседника
Регламентация процессов подразделений организации или разработка административных регламентов подразделений организации	ПСК – 5.[5] Сбор информации о процессе подразделения организации с целью разработки регламента данного процесса или административного регламента подразделения организации	Знать: - теория процессного управления; - принципы классификации процессов; -методы структурирования процессов; -основы операционного менеджмента; -методы сбора информации (наблюдения, фиксация данных, хронометраж, фотография рабочего дня, техники проведения интервью и анкетирования, анализ документов и отчетной информации, изучение обратной связи от заинтересованных сторон)	Уметь: - анализировать информацию о границах процесса, требования к процессу, цели процесса или административного регламента; -анализировать зоны ответственности, заинтересованные стороны процесса, действующие нормативы, ресурсы, входы, выходы и показатели процесса или административного регламента; -анализировать состав и последовательность операций, составляющих процесс или	Владеть навыками: - определение целей процесса подразделения организации или административного регламента подразделения организации; - определение границ процесса подразделения организации или административного регламента подразделения организации; - определение заинтересованных сторон, собственника и участников процесса подразделения организации или административного регламента подразделения организации;

[4] Профессиональный стандарт «Консультант в области развития цифровой грамотности населения (цифровой куратор)», утвержденный приказом Министерства труда и социальной защиты РФ от 31.10.2018 № 682н (трудовая функция А/02.3)

[5] Профессиональный стандарт «Специалист по процессному управлению», утвержденный приказом Министерства труда и социальной защиты РФ от 17.04.2018 № 248н (трудовая функция А/01.6)

			административный регламент; -находить необходимые документы и информацию о процессе или административном регламенте в бумажном и электронном виде в информационных системах; -выполнять наблюдения, интервью и анкетирование	-определение входов и выходов процесса подразделения организации или начала и результата выполнения административного регламента подразделения организации; -выяснение последовательности выполнения работ в процессе подразделения организации или административном регламенте подразделения организации

1.4. Категория слушателей

Программа предназначена для ветеранов боевых действий, принимавших участие (содействовавших выполнению задач) в специальной военной операции и приравненных к ним, уволенных с военной службы (службы, работы).

К освоению программы допускаются: лица, имеющие высшее образование или среднее профессиональное образование.

1.5. Формы обучения и сроки освоения

Форма обучения – очно-заочная, с применением электронного обучения и дистанционных образовательных технологий.

Срок освоения: 144 академических часов: 73 часов контактной работы с применением дистанционных образовательных технологий (ДОТ) и электронного обучения (ЭО), в том числе 2 часа итоговой аттестации, 71 часов самостоятельной контактной работы с применением электронного обучения (ЭО).

1.6. Период обучения и режим занятий

Продолжительность программы – 5 недель. Прохождение обучения складывается из контактной работы с преподавателем (вебинары), выполнения домашних заданий и самостоятельной работы.

35 дня, 5-6 дней в неделю, по 4-10 учебных часов в день.

1.7. Документ о квалификации

Вид документа, выдаваемый при успешном освоении программы - удостоверение о повышении квалификации федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации».

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Календарный учебный план

Период обучения – 35 дней						
1 день	2 день	3 день	4 день	5 день	6 день	7 день
УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	
8 день	9 день	10 день	11 день	12 день	13 день	14 день
УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	
15 день	16 день	17 день	18 день	19 день	20 день	21 день
УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	
22 день	23 день	24 день	25 день	26 день	27 день	28 день
УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	
29 день	30 день	31 день	32 день	33 день	34 день	35 день
	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ УЗ ЭО УЗ ДОТ	УЗ ЭО УЗ ДОТ ИА

Условные обозначения:

УЗ – учебные занятия.

ДОТ – это дистанционные образовательные технологии, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии слушателя и педагогического работника Академии.

ЭО – электронное обучение – это организация образовательной деятельности в электронной информационно – образовательной среде, к которой предоставляется открытый доступ слушателю через информационно – телекоммуникационную сеть «Интернет». Исключается опосредованное (на расстоянии) взаимодействие слушателя и педагогического работника Академии, используется учебно-методический материал, разработанный ими по дисциплине(модулю), который реализуется через электронную образовательную платформу.

ИА– итоговая аттестация,

УЗ ДОТ – учебные занятия с применением дистанционных образовательных технологий,

УЗ ЭО – учебные занятия с применением электронного обучения.

2.2. Учебный план

Таблица 3

Контактная работа, час.			Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий, электронного обучения), час.					Самостоятельная работа (в т.ч. электронное обучение (ЭО),	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.	Код компетенции
В том числе				Всего	В том числе								
Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
6	7	8	9	10	11	12	13	14	16	17	18	19	20
				2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
				2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
													ПСК 1

№п/п	Наименование темы	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий, электронного обучения), час.					Самостоятельная работа (в т.ч. электронное обучение (ЭО),	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
5.	Полномочия Роскомнадзора. Реестр нарушителей прав субъектов персональных данных	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
6.	Политика информационной безопасности бюджетной организации: структура, содержание, утверждение	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
7.	Разработка организационно-распорядительных документов: регламенты и инструкции	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
8.	Особенности защиты персональных данных в госучреждениях. Категории субъектов персональных данных	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
9.	Порядок проведения аттестации объектов информатизации по требованиям ФСТЭК	4	0						0					*4*				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
10.	Организация работ по лицензированию ФСТЭК и ФСБ	2	0						0					*2*				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5

№п/п	Наименование темы	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий, электронного обучения), час.					Самостоятельная работа (в т.ч. электронное обучение (ЭО),	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
11.	Типовая ИТ-инфраструктура госучреждения: серверы, АРМы, периферия	3	0						2	2				/				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
12.	Основы сетевых технологий: Ethernet, IP-адресация, DNS, DHCP	3	0						2	2				1				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
13.	Сетевая сегментация. VLAN как инструмент разделения трафика	3	0						2	2				1				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
14.	Технологии беспроводного доступа (Wi-Fi) и их уязвимости в бюджетной сфере	3	0						2	2				1				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
15.	Системы виртуализации и аспекты их безопасности	3	0						2	2				1				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
16.	Обзор актуальных киберугроз для госсектора: фишинг, ransomware, APT-атаки	3	0						2	2				1				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
17.	Классификация и источники уязвимостей программного обеспечения	3	0						2	2				1				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
18.	Основные методы и средства инженерно-	3	0						2	2				1				ПСК 1 ПСК 2

№п/п	Наименование темы	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий, электронного обучения), час.					Самостоятельная работа (в т.ч. электронное обучение (ЭО),	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
	технической защиты (ИТЗ) помещений																	ПСК 3 ПСК 4 ПСК 5
19.	Основы криптографии: шифрование, ЭЦП, хэш-функции	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
20.	Средства криптографической защиты информации (СКЗИ). Ключевые носители	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
21.	Защищенные VPN-каналы. Протоколы и принципы построения	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
22.	Системы защиты от несанкционированного доступа: принципы работы, типы, политики доступа.	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
23.	Современные средства антивирусной защиты для бюджетных организаций	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
24.	Системы обнаружения и предотвращения вторжений (IDS/IPS)	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
25.	Системы контроля доступа (СКУД) и видеонаблюдение (СОТ). Интеграция с	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5

№п/п	Наименование темы	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий, электронного обучения), час.					Самостоятельная работа (в т.ч. электронное обучение (ЭО),	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
	информационной безопасностью																	
26.	Принципы мониторинга информационной безопасности	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
27.	Методики оценки защищенности информационной безопасности	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
28.	Первоначальные действия при обнаружении инцидента: локализация, сбор информации	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
29.	Ручная проверка на уязвимости	5	0						2	2				3				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
30.	Документирование инцидентов. Заполнение формы уведомления для ФСТЭК (по ФЗ-187)	6	0						2	2				4				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
31.	Пост-инцидентный анализ. Составление итогового отчета и план устранения причин	2	0						0					2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
32.	Клиентоориентированный сервис и этапы	4	0						2	2				2				ПСК 1 ПСК 2

№п/п	Наименование темы	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий, электронного обучения), час.					Самостоятельная работа (в т.ч. электронное обучение (ЭО),	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
	продаж																	ПСК 3 ПСК 4 ПСК 5
33.	Этика делового общения	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
34.	Навыки самопрезентации. Составление резюме сотрудника по защите информации	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
35.	Подготовка к собеседованию: типовые вопросы и кейсы	5	0						3	3				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
36.	Адаптация и развитие в коллективе. Управление личной эффективностью	6	0						4	4				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
37.	Карьерные возможности в госсекторе. Адаптационный семинар: переход к гражданской профессии	4	0						2	2				2				ПСК 1 ПСК 2 ПСК 3 ПСК 4 ПСК 5
38.	Итоговая аттестация (экзамен в форме тестирования)	2	0						0								2	
ВСЕГО:		**144**							**71**	**71**				**71**			**2**	

2.3. Содержание программы по темам

Номер темы и наименование	Содержание темы
Тема 1. Введение в профессию. Трудовые функции специалиста по защите информации	Понятие и содержание профессиональ специалиста по защите информации бюджетной сферы. Место и роль защите информации в структур Квалификационные требования к спец профессиональным стандартам и кв справочникам. Основные трудс специалиста. Права, обязанности и специалиста.
Тема 2. Нормативно-правовое регулирование деятельности в области защиты информации. Федеральный закон №152-ФЗ «О персональных данных», Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	Правовые основы информационной Конституции РФ. Общие положения и информационной безопасности. Федер 27.07.2006 № 149-ФЗ «Об информационных технологиях и информации». Федеральный закон от 2 ФЗ «О персональных данных». Федер 26.07.2017 № 187-ФЗ «О безопасно информационной инфраструктуры Федерации». Иерархия подзаконн правовых актов (указы Президента РФ Правительства РФ, приказы регулятор
Тема 3. Требования ФСТЭК России к информационной безопасности (Приказы № 17, 21, 31, 239).	Общие положения и значение треб России в системе информационной б Роль ФСТЭК России как регулятора информации. Место приказов № 17 иерархии нормативно-правовых актов регулирования, взаимосвязь с законодательством, применение на пра
Тема 4. Требования ФСБ России в области защиты информации (Приказы № 378, 117, 66)	Общие положения и роль ФС информационной безопасности РФ полномочия ФСБ как регулятора в информации. Понятие и сфера примен 378, 117, 66. Основные требовани направлениям защиты. Порядок реали на практике.
Тема 5. Полномочия Роскомнадзора. Реестр нарушителей прав субъектов персональных данных	Федеральная служба по надзору информационных технологий коммуникаций как уполномоченный прав субъектов персональных да статус, основные функции и полномо надзор за соответствием обработк данных требованиям законодательс нарушителей прав субъектов персон порядок формирования и ведения, включения, порядок исключения из ре
Тема 6. Политика информационной безопасности бюджетной организации: структура, содержание, утверждение	Политика информационной без основополагающий внутренний документ, определяющий цели, зада направления деятельности организа обеспечения информационной Нормативная основа разработки поли политики информационной безопасно разработки политики для бюджетн Порядок утверждения политики.

Номер темы и наименование	Содержание темы
Тема 7. Разработка организационно-распорядительных документов: регламенты и инструкции	Иерархия документов в системе организационно-распорядительной документации по информационной безопасности. Положение о защите персональных данных. Инструкция пользователя информационной системы. Регламент резервного копирования и восстановления данных. Инструкция по антивирусной защите. Регламент реагирования на инциденты информационной безопасности. Требования к оформлению документов. Порядок введения в действие, ознакомления сотрудников, хранения.
Тема 8. Особенности защиты персональных данных в госучреждениях. Категории субъектов персональных данных	Специфика обработки персональных данных в государственных и муниципальных учреждениях. Особый правовой статус государственных информационных систем (ГИС) и муниципальных информационных систем (МИС). Категории субъектов персональных данных в бюджетной сфере. Особенности обработки специальных категорий персональных данных. Особенности обработки биометрических персональных данных. Обязанность уведомления Роскомнадзора о начале обработки персональных данных. Ответственность за нарушения в области обработки персональных данных.
Тема 9. Порядок проведения аттестации объектов информатизации по требованиям ФСТЭК	Понятие аттестации объектов информатизации. Цели и задачи аттестации. Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну». Объекты, подлежащие обязательной аттестации. Этапы проведения аттестации и участники процесса. Ответственность за эксплуатацию неаттестованных систем.
Тема 10. Организация работ по лицензированию ФСТЭК и ФСБ	Понятие лицензирования отдельных видов деятельности. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности». Лицензирование деятельности по технической защите конфиденциальной информации (ФСТЭК России). Лицензирование деятельности по разработке, производству, распространению шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации (ФСБ России). Особенности лицензирования для бюджетных организаций.
Тема 11. Типовая ИТ-инфраструктура госучреждения: серверы, АРМы, периферия	Понятие ИТ-инфраструктуры государственного учреждения: состав, назначение, основные компоненты. Серверный сегмент: классификация серверов. Требования к размещению серверного оборудования. Автоматизированные рабочие места: типовая конфигурация, программное обеспечение. Особенности перехода на отечественное ПО. Периферийное оборудование: принтеры, МФУ, сканеры. Сетевое оборудование: коммутаторы, маршрутизаторы, точки доступа. Системы хранения данных: локальные диски, сетевые хранилища. Требования к резервированию и отказоустойчивости.

Номер темы и наименование	Содержание темы
Тема 12. Основы сетевых технологий: Ethernet, IP-адресация, DNS, DHCP	Введение в сетевые технологии. Ключевые понятия: сеть, узел, протокол, стек протоколов. Принципы работы и стандарты технологии Ethernet. Понятие IP-адреса, структура и классы адреса. Частные и публичные IP-адреса. Особенности IP-адресации в бюджетных организациях. Назначение и принцип работы протокола DHCP. Настройка DHCP-сервера, пулы адресов, резервирование. Система доменных имен DNS: назначение, иерархическая структура. Домены и зоны. Типы ресурсных записей. Принцип разрешения имен.
Тема 13. Сетевая сегментация. VLAN как инструмент разделения трафика	Понятие сегментации сети, цели и задачи сегментации. Основные методы сегментации. Понятие широковещательного домена. Проблемы плоских сетей. Технология VLAN: основы и принцип работы. Преимущества использования VLAN. Стандарты и протоколы. Типы VLAN. Настройка и управление VLAN. Взаимодействие VLAN с сетевыми уровнями. Безопасность и защита с помощью VLAN.
Тема 14. Технологии беспроводного доступа (Wi-Fi) и их уязвимости в бюджетной сфере	Стандарты Wi-Fi: эволюция, скорости передачи, частотные диапазоны. Протоколы безопасности беспроводных сетей. Основные уязвимости Wi-Fi. Инструменты тестирования безопасности Wi-Fi. Особенности организации Wi-Fi в бюджетных учреждениях. Защита от основных угроз.
Тема 15. Системы виртуализации и аспекты их безопасности	Понятие виртуализации: цели, преимущества (консолидация ресурсов, изоляция, гибкость управления). Типы виртуализации: серверная, сетей, рабочих столов. Компоненты виртуализированной среды. Российский рынок виртуализации: импортозамещение, требования к использованию сертифицированных средств виртуализации для субъектов КИИ и госорганов. Основные угрозы безопасности виртуализации. Меры защиты виртуализированных сред. Требования регуляторов: приказ ФСТЭК России № 187.
Тема 16. Обзор актуальных киберугроз для госсектора: фишинг, ransomware, APT-атаки	Современный ландшафт киберугроз для госсектора: рост числа атак, смещение фокуса на нанесение максимального ущерба. Фишинг: определение, виды, техники обхода защиты и меры защиты. Программы-вымогатели (ransomware): понятие, принцип действия, механизмы и противодействие атаки. Понятие, характеристики и методы APT-атаки.
Тема 17. Классификация и источники уязвимостей программного обеспечения	Понятие уязвимости информационной системы. Отличие уязвимости от угрозы и риска. Классификация уязвимостей. Источники информации об уязвимостях. Причины возникновения уязвимостей в программном обеспечении. Управление уязвимостями: выявление, оценка критичности, приоритезация, контроль.
Тема 18. Основные методы и средства инженерно-технической защиты (ИТЗ) помещений	Понятие инженерно-технической защиты информации. Физическая защита периметра и помещений. Технические каналы утечки информации и методы защиты. Системы видеонаблюдения. Организационные меры ИТЗ. Особенности ИТЗ в бюджетных организациях. Аттестация помещений по требованиям безопасности.

Номер темы и наименование	Содержание темы
Тема 19. Основы криптографии: шифрование, ЭЦП, хэш-функции	Понятие криптографии и основные задачи криптографической защиты в бюджетных организациях. Шифрование как процесс преобразования информации с целью сокрытия от несанкционированного доступа. Понятие, свойства и назначение хэш-функций. Понятие и назначение электронной цифровой подписи. Виды электронных подписей согласно ФЗ № 63. Применение криптографии в бюджетных организациях.
Тема 20. Средства криптографической защиты информации (СКЗИ). Ключевые носители	Понятие и виды СКЗИ. Классификация ключевой информации. Ключевые носители. Правила эксплуатации СКЗИ в бюджетной организации. Понятие компрометации ключей. Учет СКЗИ и ключевых документов.
Тема 21. Защищенные VPN-каналы. Протоколы и принципы построения	Понятие VPN. Обеспечение конфиденциальности, целостности и аутентификации трафика. Типовые конфигурации VPN. Протоколы построения VPN-соединений. Отечественные решения для построения VPN. Применение VPN в бюджетных организациях. Требования безопасности при эксплуатации VPN.
Тема 22. Системы защиты от несанкционированного доступа: принципы работы, типы, политики доступа.	Понятие несанкционированного доступа (НСД) к информации. Системы защиты от НСД. Основные компоненты СЗИ от НСД. Типы СЗИ от НСД. Механизмы разграничения доступа. Требования ФСТЭК России к СЗИ от НСД. Политики доступа в бюджетных организациях.
Тема 23. Современные средства антивирусной защиты для бюджетных организаций	Понятие вредоносного программного обеспечения: классификация (вирусы, черви, трояны, шпионское ПО, программы-вымогатели, рекламное ПО). Актуальные угрозы для госсектора. Принципы работы антивирусных средств. Критерии выбора антивирусных средств для бюджетных организаций. Обзор антивирусных решений. Организация антивирусной защиты в бюджетной организации. Инструкция по антивирусной защите как организационно-распорядительный документ.
Тема 24. Системы обнаружения и предотвращения вторжений (IDS/IPS)	Понятие систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS). Цели и задачи: выявление фактов несанкционированного доступа, сетевых атак, вредоносной активности. Отличия IDS от IPS. Классификация систем обнаружения вторжений. Архитектура IDS/IPS. Методы анализа трафика. Размещение IDS/IPS в инфраструктуре. Требования ФСТЭК России.
Тема 25. Системы контроля доступа (СКУД) и видеонаблюдение (СОТ). Интеграция с информационной безопасностью	Понятие физической безопасности объекта. Роль СКУД и систем охранного телевидения (СОТ) в обеспечении комплексной безопасности бюджетной организации. Системы контроля и управления доступом (СКУД): назначение, компоненты, виды доступа. Системы охранного телевидения (СОТ, видеонаблюдение): назначение, типы камер, характеристики, хранение архива. Интеграция СКУД и СОТ с информационной безопасностью. Требования к защите информации в СКУД и СОТ.
Тема 26. Принципы мониторинга информационной безопасности	Понятие и цели мониторинга информационной безопасности. Нормативно-правовая основа

Номер темы и наименование	Содержание темы
	мониторинга. Уровни мониторинга. Принципы эффективного мониторинга. Определение объектов и параметров мониторинга. Метрики эффективности мониторинга (KPI). Интеграция мониторинга с системами реагирования на инциденты и процессами управления уязвимостями. Документирование результатов мониторинга. Требования к хранению и защите результатов мониторинга.
Тема 27. Методики оценки защищенности информационной безопасности	Подходы к определению понятия оценки защищенности информационной безопасности. Классификация методов оценки защищенности. Эталонные модели и стандарты для оценки. Процесс оценки защищенности. Методы технического анализа. Оценка организационных мер. Периодичность оценки и документирование результатов.
Тема 28. Первоначальные действия при обнаружении инцидента: локализация, сбор информации	Сущность понятия «инцидент информационной безопасности». Классификация инцидентов по источникам и последствиям. Модель жизненного цикла реагирования при обнаружении инцидента. Типичные ошибки при первоначальном реагировании. Взаимодействие с ГосСОПКА.
Тема 29. Ручная проверка на уязвимости	Суть ручной проверки на уязвимости как метода анализа защищённости информационных систем. Отличие от автоматизированного сканирования. Области применения ручной проверки. Методы ручной проверки. Инструменты для ручной проверки. Ограничения ручной проверки.
Тема 30. Документирование инцидентов. Заполнение формы уведомления для ФСТЭК (по ФЗ-187)	Цели документирования инцидентов. Состав документируемой информации по инциденту. Внутренние формы документирования. Уведомление ФСТЭК России об инцидентах на объектах КИИ. Состав информации в уведомлении ФСТЭК. Уведомление Роскомнадзора. Требования к защите информации о расследуемых инцидентах: конфиденциальность, ограниченный доступ, целостность.
Тема 31. Пост-инцидентный анализ. Составление итогового отчета и план устранения причин	Суть и значение пост-инцидентного анализа. Цели пост-инцидентного анализа. Ключевые принципы анализа. Этапы проведения анализа. Структура итогового отчета по инциденту. Разработка плана устранения причин. Инструменты и шаблоны. Типичные ошибки при составлении итогового отчета и плана устранения причин.
Тема 32. Клиентоориентированный сервис и этапы продаж	Понятие клиентоориентированного сервиса: ценности, принципы, отличия от формального обслуживания. Сегментация аудитории и выявление явных и скрытых потребностей. Карта пути клиента. Сбор и анализ обратной связи. Ключевые метрики: NPS, CSAT, уровень удержания клиентов. Этапы продаж: классическая модель и современные адаптации. Инструменты и техники продаж.
Тема 33. Этика делового общения	Понятие деловой этики и ее значение в профессиональной деятельности специалиста по защите информации. Основные принципы делового общения. Нормы и правила делового этикета. Управление эмоциями в деловом общении: эмоциональный

Номер темы и наименование	Содержание темы
	интеллект, саморегуляция, эмпатия. Поведение в конфликтных ситуациях.
Тема 34. Эффективная презентация продукта через выгоды и особенности	Презентация как инструмент коммуникации. Виды презентации. Особенности презентации технических решений и услуг в области защиты информации. Структура убедительной презентации. Адаптация презентации под аудиторию. Визуализация презентации: принципы создания слайдов, инфографика, демонстрация работы продукта.
Тема 35. Навыки самопрезентации. Составление резюме сотрудника по защите информации	Понятие и цели самопрезентации. Управление впечатлением о себе в профессиональной среде. Структура эффективного резюме специалиста по защите информации. Распространенные ошибки при составлении резюме. Дополнительные инструменты самопрезентации.
Тема 36. Подготовка к собеседованию: типовые вопросы и кейсы	Этапы подготовки к собеседованию. Типовые вопросы на собеседовании для специалистов по защите информации. Профессиональные кейсы. Методика ответа на сложные вопросы и кейсы. Непрофессиональные вопросы (проверка soft skills). Подготовка вопросов к работодателю. Правила поведения на собеседовании: пунктуальность, внешний вид, уверенное поведение, умение слушать, позитивный настрой.
Тема 37. Адаптация и развитие в коллективе. Управление личной эффективностью	Понятие и виды адаптации сотрудника в организации. Отличие профессиональной адаптации от социально-психологической. Этапы адаптации нового сотрудника. Факторы успешной адаптации. Построение профессиональных отношений. Обратная связь как инструмент развития. Управление личной эффективностью: тайм-менеджмент, управление стрессом и профилактика профессионального выгорания, постановка личных и профессиональных целей, непрерывное обучение и повышение квалификации.
Тема 38. Карьерные возможности в госсекторе. Адаптационный семинар: переход к гражданской профессии	Обзор карьерных возможностей для специалистов по защите информации в государственном секторе. Специфика работы в госсекторе. Требования к специалистам в госсекторе. Источники поиска вакансий в госсекторе. Перспективы карьерного роста. Психологическая подготовка к смене профессиональной среды: принятие изменений, работа с ожиданиями, формирование новых профессиональных связей.

[ИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Кадровое обеспечение

Сведения о профессорско-преподавательском составе

Таблица 7

я	Дополнительн/ая/ые квалификаци/я/и	Место работы, должность, основное/дополнительное место работы	Ученая степень, ученое (почетное) звание	Стаж работы в области профес-сиональной деятельности/ по дополнительной квалификации	Стаж научно-педагогической работы		Наименование читаемой дисциплины (модуля), практики/стажировки (при наличии) по данной программе
					Всего	В том числе п читаемой дисциплине (модулю)	
я	Программа ПК РАНХиГС «Использование СДО в образовательном процессе с применением электронного обучения и дистанционных образовательных технологий» (2021)	заместитель директора ЮРИУ РАНХиГС, старший преподаватель кафедры менеджмента	-	21	21	13	
?ТУ),	Программа ПК РАНХиГС «Использование СДО в образовательном процессе с применением электронного обучения и дистанционных образовательных технологий» (2021) Программа ПК РАНХиГС «Маркетинг образования: продвижение образовательной организации на международном рынке образовательных услуг (с учетом региональных особенностей)» (2020)	директор учебно-научного центра, доцент сектора реализации национальных программ и федеральных проектов центра дополнительного образования ЮРИУ РАНХиГС	к.эконом.н.	21	21	21	
	Программа ПК РАНХиГС						

Бурлаков Михаил Валерьевич	ФГОУ ВПО «СКАГС», Государственное и муниципальное управление	Программа ПК РАНХиГС «Основы бережливого управления (для преподавателей)» (2024), «Тренинг для тренеров: методология и проведение обучения в формате тренинга» (2023)	директор центра молодежных инициатив, преподаватель сектора реализации национальных программ и федеральных проектов центра дополнительного образования ЮРИУ РАНХиГС	-	14	2	2	
Шлеверда Иван Николаевич	Федеральное государственное образовательное учреждение высшего профессионального образования Северо-Кавказская академия государственной службы, специалист	Развитие компетенций в сфере регионального и муниципального управления по направлениям современные ИКТ в ГМУ и институциональные основы МСУ, 2021; Преподаватель в цифровой образовательной среде (электронная информационно-образовательная среда в ВУЗе), 2021; Профилактика распространения в образовательных организациях радикальной и иной деструктивной идеологии, 2021; Актуальная политическая повестка, 2022; Социокультурная среда и психолого-педагогическое сопровождение обучающихся инвалидов в образовательных организациях профессионального образования, 2022;	Южно-Российский институт управления – филиал РАНХиГС, директор центра дополнительного образования, доцент кафедры государственного и муниципального управления, доцент сектора реализации национальных программ и федеральных проектов центра дополнительного образования Почасовая оплата	Кандидат политических наук, доцент	8	8	2	
Яланский Александр Павлович	Высшее образование Экономическая теория Экономист, преподаватель экономических дисциплин	"Интернет-маркетинг" по профилю направления подготовки 38.03.02. "Менеджмент" на основе профессионального стандарта "Специалист по продвижению и распространению продукции средств массовой информации", 2020; Социокультурная среда и психолого-педагогическое сопровождение обучающихся инвалидов в образовательных	доцент кафедры менеджмента Южно-Российского института управления – филиала РАНХиГС	к. э. н., доцент	22	22	5	

		организациях профессионального образования, 2022						
Санин Алексей Сергеевич	Донской государственный технологический университет, Экономика и управление	-	Директор программы центра дополнительного образования ЮРИУ РАНХиГС	к. э. н.	16	3	3	
Кислицкая Наталья Александровна	Северо-Кавказскую академию государственной службы	менеджер-экономист по специальности «Государственное и муниципальное управление»; Дополнительная квалификация (к высшему образованию) «Переводчик в сфере профессиональной коммуникации»; кандидат экономических наук, 22.10.2007 г., доцент, 22.01.2015 г.	Доцент кафедры экономики, финансов и природопользования	к. э. н.				
Котлярова Ольга Владимировна	Владимирский государственный педагогический институт. Специальность «Филология» (специалитет). РАНХиГС по направлению «Государственное и муниципальное управление» (магистратура)	Программа ПК РАНХиГС «Использование СДО в образовательном процессе с применением электронного обучения и дистанционных образовательных технологий» (2020)	Владимирский филиал РАНХиГС, доцент, внешний	к.фил.н	21	21	8	

Реализация дополнительной профессиональной программы повышения квалификации обеспечивается профессорско-преподавательским составом РАНХиГС. Научно-педагогические кадры, реализующие программу, имеют специальную подготовку, базовое образование, соответствующее профилю преподаваемой дисциплины (модуля), и систематически занимаются научно-методической деятельностью. Реализация образовательной программы осуществляется педагогическими кадрами, имеющими высшее образование, соответствующее профилю преподаваемой дисциплины (модуля).

3.2. Материально-техническое и программное обеспечение реализации программы

Южно-Российский институт управления – филиал РАНХиГС обеспечивает слушателей необходимой материально-технической базой, соответствующей действующим санитарным и противопожарным правилам и нормам (при проведении очных занятий по программе):

- учебные аудитории с возможностью использования преподавателем мультимедийного проектора, ноутбука или стационарного компьютера, средства звуковоспроизведения, экрана, флипчарта, обычной или электронной доски и маркеров, доступа к беспроводным сетям Wi-Fi с выходом в Интернет для проведения занятий лекционного-практического типа, групповых и индивидуальных консультаций и промежуточной аттестации, в том числе с применением дистанционных образовательных технологий
- помещения для проведения практических занятий, оборудованными учебной мебелью;
- библиотека, имеющую рабочие места для слушателей, оснащенные компьютерами с доступом к базам данных и сети Интернет;
- компьютерные классы.

Реализуемая программа повышения квалификации обеспечена всеми необходимыми материально-техническими ресурсами. На весь период обучения слушателям предоставляются:

– учебные и учебно-методические материалы: разработанная дополнительная профессиональная программа повышения квалификации, учебно- методический комплекс, информационно-методические материалы по образовательной программе, в том числе в электронном виде;

– доступ к библиотечному фонду, современным профессиональным базам данных и информационным справочным правовым системам, а также к автоматизированным системам хранения и поиска информации;

– доступ к платформе СДО: https://uriu.gosedu.ru;

– техническая поддержка.

Слушатели получают методическую поддержку в процессе обучения и по заверении обучения, в т.ч. имеют возможность получать консультации по электронной почте у преподавателей, принимающих участие в обучении.

Реализация программы в дистанционном режиме осуществляется через Систему дистанционного обучения https://uriu.gosedu.ru. Слушателям предоставляется авторизованный доступ на информационно-образовательный портал https://uriu.gosedu.ru через ввод логина и пароля. Логин и пароль присваивается администратором системы дистанционного обучения.

Дистанционное обучение включает в себя изучение материалов, прохождение электронных курсов на информационно-образовательном портале https://uriu.gosedu.ru.

Для работы в рамках реализации программы требуется:

1. Рабочее место обучающегося при освоении программы с использованием дистанционных технологий и/или электронного обучения должно быть организовано по месту его пребывания и соответствовать необходимым нормативам и требованиям, быть оборудовано компьютером, имеющим доступ к сети Интернет, монитором, клавиатурой, колонками, рабочей поверхностью.

2. Рабочее место преподавателя при работе в рамках реализации программы с использованием дистанционных технологий должно быть организовано по месту его пребывания и соответствовать необходимым нормативам и требованиям, быть оборудовано компьютером, имеющим доступ к сети Интернет, монитором, клавиатурой, колонками, рабочей поверхностью.

3. Для проведения лекций при очной форме обучения требуются аудитории, оснащенные проекторами, оборудованные микрофонами. Для проведения практических занятий при очной форме обучения, требуются аудитории, оборудованные столами, стульями, маркерными/меловыми досками».

3.3 Учебно-методическое и информационное обеспечение программы

Содержание обучения по образовательной программе связано с его средой таким образом, чтобы учебная среда стала не отвлекающим, а вспомогательным фактором процесса обучения.

Дополнительная профессиональная программа обеспечивается необходимой учебной, учебно-методической литературой и библиотечно-информационными ресурсами.

Электронно-библиотечная система обеспечивает возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ в сети Интернет.

Одним из условий успешности дополнительного профессионального образования является активная позиция каждого слушателя, поэтому освоение содержания программы предполагается в деятельностном режиме.

Преподавание данной дополнительной профессиональной программы повышения квалификации различным категориям слушателей требует обособления методического обеспечения, детализирующего и уточняющего содержание программы в зависимости от возрастных, психофизиологических, социальных и иных особенностей целевой аудитории.

Самостоятельная работа

Слушатели самостоятельно изучают материалы, расположенные на платформе https://uriu.gosedu.ru/.

Примерные задания для самостоятельной работы

Изучить электронные курс по теме «Специалист по защите информации в организациях бюджетной сферы»

Примерный перечень заданий для самостоятельной работы

Задание 1.

Часть 1. Нормативно-организационная

Определите категории обрабатываемых ПДн в соответствии с ФЗ-152 и Постановлением Правительства №1119.

1. **Определите требуемый уровень защищенности (УЗ) ПДн** для данной информационной системы.

2. **Составьте перечень недостающих организационно-распорядительных документов** (не менее 5 наименований), которые необходимо разработать в поликлинике.

3. **Разработайте фрагмент Политики обработки ПДн** (раздел «Цели обработки ПДн» и раздел «Меры по обеспечению безопасности ПДн»).

4. **Составьте модель угроз безопасности ПДн** для АИС (краткую — выделите не менее 5 актуальных угроз с обоснованием).

Часть 2. Техническая (выполняется самостоятельно, 2 часа)

1. **Предложите архитектурное решение** по сегментации сети: нарисуйте схему, на которой укажите:
   - Размещение сервера БД;
   - Размещение АРМ пользователей;
   - Межсетевой экран (где и какие правила);
   - Организацию VPN для главного врача;
   - Систему резервного копирования.
2. **Подберите состав средств защиты информации (СЗИ)**, необходимых для приведения системы в соответствие с требованиями:
   - СКЗИ (какие и для чего);
   - Средства антивирусной защиты;
   - Межсетевые экраны;
   - Системы обнаружения вторжений (IDS/IPS);
   - Средства защиты от НСД. *Для каждого типа СЗИ укажите конкретную функцию в данной системе.*
3. **Составьте смету (ориентировочную)** минимально необходимых закупок (в свободной форме, без привязки к конкретным ценам, но с указанием типов продуктов).
4. **Подготовьте план первоочередных мероприятий** на 3 месяца с указанием ответственных и сроков.

Задание 2.

Легенда (вводная)

Вы — сотрудник отдела информационной безопасности **Департамента образования администрации г. N-ска** (бюджетное учреждение, объединяющее 45 школ и 12 детских садов).

Хронология событий:

08:00, понедельник. Системный администратор одной из школ (МБОУ СОШ №7) сообщает, что учителя не могут открыть электронный журнал. При попытке входа на сайт школы отображается странное сообщение на английском языке с требованием выкупа в биткоинах.

09:15. Выясняется, что заражены:
- Сервер электронного журнала (ОС Windows Server 2012);
- 12 учительских ноутбуков;
- Компьютер директора школы.

Все зараженные машины заблокированы, файлы зашифрованы (расширение .encrypted).

09:45. Учитель информатики сообщает, что в пятницу вечером (в 18:30) открывал подозрительное письмо «От департамента образования — срочный приказ» с вложением «Приказ_№45.docm» и макросы были включены.

10:00. Выясняется, что:
- В школе не было сегментации сети (сервер и АРМы в одной подсети);
- Резервное копирование не работало 2 недели (закончилось место на диске);
- Антивирус был установлен, но сигнатуры обновлялись вручную раз в месяц;

- Учетная запись директора имела права локального администратора на всех машинах.

12:00. Директор школы требует срочно восстановить работу. Мэр города поставлен в известность. Ситуация на контроле у прокуратуры.

Входящие материалы (выдаются слушателям):

1. Дамп письма с фишингом (текст, вложение).
2. Выдержка из логов межсетевого экрана за пятницу-понедельник.
3. Форма уведомления ФСТЭК о компьютерном инциденте (Приказ ФСТЭК №135).
4. Форма уведомления Роскомнадзора об утечке ПДн (Приказ Роскомнадзора №178).

Задание

Этап 1. Анализ и локализация

Распределите роли в команде:

- **Руководитель расследования** — координирует, принимает решения;
- **Технический аналитик** — работает с логами, определяет вектор атаки;
- **Специалист по документам** — готовит документацию для регуляторов;
- **Специалист по коммуникациям** — готовит объяснения для руководства.

Задачи этапа:

1. Проанализируйте фишинговое письмо и вложение (на основе описания или учебного файла). Определите признаки вредоносности.
2. Проанализируйте логи межсетевого экрана. Определите:
   - Была ли подозрительная активность (исходящие соединения на неизвестные IP);
   - Когда произошло первое заражение.
3. Оцените масштаб инцидента: какие данные могли быть скомпрометированы (в школе обрабатываются ПДн учащихся, включая данные свидетельств о рождении, СНИЛС, адреса, медицинские справки).
4. Примите решение о дальнейших действиях:
   - Отключить ли зараженный сегмент сети?
   - Сообщать ли в правоохранительные органы?
   - Требуется ли эвакуация непораженных данных?

Нормативно-правовые документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
2. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
4. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.
5. Приказ ФСТЭК РФ «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25.12.2017 № 239.
6. Приказ ФСТЭК РФ «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных

объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 14.03.2014 № 31.

7. Приказ ФСТЭК РФ «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 № 21.

8. Приказ ФСТЭК РФ «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11.02.2013 № 17.

9. Приказ ФСТЭК России «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» от 29.04.2021 № 77.

10. Приказ ФСБ РФ «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» от 10.07.2014 № 378.

11. Приказ ФСБ РФ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» от 09.02.2005 № 66.

12. Приказ ФСБ РФ «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств» от 18.03.2025 № 117.

Основная литература

1. Абельская, Р. Ш. Теория и практика делового общения для IT-направлений : учебник для вузов / Р. Ш. Абельская ; под научной редакцией И. Н. Обабкова. — Москва : Издательство Юрайт, 2025. — 95 с. — (Высшее образование). — ISBN 978-5-534-17872-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/564677

2. Баланов, А. Н. Цифровая трансформация государственного сектора. Интеграция, управление и безопасность : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 328 с. — ISBN 978-5-507-49310-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/417749

3. Вавилин, Я. А. Информационные технологии в управлении качеством и защита информации : учебное пособие для вузов / Я. А. Вавилин, В. Г. Солдатов, И. Г. Манкевич. — Санкт-Петербург : Лань, 2025. — 196 с. — ISBN 978-5-507-51437-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/447242

4. Внуков А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584050

5. Войниканис, Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом : учебник для вузов / Е. А. Войниканис ; под редакцией М. А. Федотова. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 50 с. — (Высшее образование). — ISBN 978-5-534-19364-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589232

6. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588741

7. Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/586060

8. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590420

9. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2026. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583156

10. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров, А. С. Никифорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/288974

11. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583236

12. Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 6-е изд., стер. — Санкт-Петербург : Лань, 2025. — 124 с. — ISBN 978-5-507-52899-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/462293

13. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 427 с. — (Высшее образование). — ISBN 978-5-534-18043-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/582668

14. Тумбинская, М. В. Защита информации на предприятии : учебное пособие для вузов / М. В. Тумбинская, М. В. Петровский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 184 с. — ISBN 978-5-507-52967-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/463043

15. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2026. — 349 с. — (Высшее

образование). — ISBN 978-5-534-19762-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583858

Дополнительная литература

1. Аникин Д. Потенциальные угрозы, исходящие от ИИ-сервисов // Обзор.НЦПТИ. 2025. №3 (42). URL: https://cyberleninka.ru/article/n/potentsialnye-ugrozy-ishodyaschie-ot-ii-servisov

2. Аррыкова Г.К., Аширов И.Г., Язбердиева А.Я., Юзбашыева Д.Д. Кибератаки на сетевые протоколы: методы обнаружения и предотвращения // Наука и мировоззрение. 2025. №39. URL: https://cyberleninka.ru/article/n/kiberataki-na-setevye-protokoly-metody-obnaruzheniya-i-predotvrascheniya

3. Арустамян Г. В., Шестак Д. О., Дилбандян Р. А., Терещенко О. В. Российские информационные вызовы и ответы на них // Культура мира. 2025. №4 (47). URL: https://cyberleninka.ru/article/n/rossiyskie-informatsionnye-vyzovy-i-otvety-na-nih

4. Бабина Д. А. Актуальные проблемы работы с персональными данными в Российской Федерации // Инновационная наука. 2024. №3-2. URL: https://cyberleninka.ru/article/n/aktualnye-problemy-raboty-s-personalnymi-dannymi-v-rossiyskoy-federatsii

5. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715

6. Брычеев А.С. Применение искусственного интеллекта в органах государственной власти: вызовы и перспективы // Вестник евразийской науки. 2024. №6S. URL: https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-v-organah-gosudarstvennoy-vlasti-vyzovy-i-perspektivy

7. Васильев А. Краткая история эволюции кибератак // МНИЖ. 2023. №11 (137). URL: https://cyberleninka.ru/article/n/kratkaya-istoriya-evolyutsii-kiberatak

8. Джурук Д.С., Коршунов А.В., Пушечников А.А. Защита персональных данных в эпоху больших данных // Право и государство: теория и практика. 2025. №4. URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-epohu-bolshih-dannyh

9. Корецкий В.П, Пинчук Д.В. Обеспечение информационной безопасности на предприятиях государственного сектора с учетом изменения нормативно-правовой базы и актуальных угроз кибербезопасности // Вестник евразийской науки. 2025. №5. URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-na-predpriyatiyah-gosudarstvennogo-sektora-s-uchetom-izmeneniya-normativno-pravovoy-bazy

10. Корягина, Н. А. Самопрезентация и убеждающая коммуникация : учебник и практикум для вузов / Н. А. Корягина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 378 с. — (Высшее образование). — ISBN 978-5-534-16070-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587082

11. Назарян А. К., Карцан И. Н. Современные кибератаки: классификация и способы защиты // Информатика. Экономика. Управление / Informatics. Economics. Management. 2025. №1. URL: https://cyberleninka.ru/article/n/sovremennye-kiberataki-klassifikatsiya-i-sposoby-zaschity

12. Попкова А.А., Парфенов К.В., Алборов А.Р. Угрозы информационной безопасности в государственном секторе России // Известия вузов. Социология. Экономика. Политика. 2024. №4. URL: https://cyberleninka.ru/article/n/ugrozy-informatsionnoy-bezopasnosti-v-gosudarstvennom-sektore-rossii

13. Чернышова, Л. И. Этика, культура и этикет делового общения : учебник для вузов / Л. И. Чернышова. — Москва : Издательство Юрайт, 2025. — 158 с. — (Высшее

образование). — ISBN 978-5-534-16621-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561128

14. Шанепесова С., Пенаева О., Джанмырадов М., Башиммырадов О. Риски кибератак на критическую инфраструктуру и методы их предотвращения // Символ науки. 2024. №11-1-1. URL: https://cyberleninka.ru/article/n/riski-kiberatak-na-kriticheskuyu-infrastrukturu-i-metody-ih-predotvrascheniya

15. Шубинский, М. И. Информационная безопасность для работников бюджетной сферы. Защита персональных данных : учебное пособие / М. И. Шубинский. — Санкт-Петербург : НИУ ИТМО, 2023. — 77 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/70858

Интернет-источники

1. Банк России: www.cbr.ru
2. Агентство по страхованию вкладов (АСВ): www.asv.org.ru
3. Национальная система платежных карт (НСПК, ПС «Мир»): www.nspk.ru
4. Финансовая культура (проект Банка России): fincult.info

Информационные базы

1. Поисковая система нормативных правовых актов «Гарант» [Электронный ресурс]. Режим доступа: www.garant.ru
2. Поисковая система нормативных правовых актов «Консультант+» [Электронный ресурс]. Режим доступа: www.consultant.ru
3. JSTOR [Электронный ресурс]. Режим доступа: http://ezproxy.ranepa.ru:3561/login?url=http://www.jstor.org
4. Science Direct [Электронный ресурс]. Режим доступа: http://ezproxy.ranepa.ru:3561/login?url=http://www.sciencedirect.com/
5. Oxford Journals [Электронный ресурс]. Режим доступа: http://ezproxy.ranepa.ru:3561/login?url=http://www.oxfordjournals.org/
6. Web of Science (WoS) [Электронный ресурс]. Режим доступа: http://ezproxy.ranepa.ru:3561/login?url=http://www.webofknowledge.com
7. Polpred.com Обзор СМИ [Электронный ресурс]. Режим доступа: http://polpred.com/news
8. ПравоИнформ [Электронный ресурс]. Режим доступа: http://www.base.spinform.ru/index.fwx
9. ЭБС IPRbooks [Электронный ресурс]. Режим доступа: http://www.iprbookshop.ru
10. ЭБС издательства ЮРАЙТ [Электронный ресурс]. Режим доступа: http://www.biblio-online.ru/home;jsessionid=8a54e6204214e246766a3b2dafb9?0
11. Электронная библиотека Издательского дома «Гребенников» [Электронный ресурс]. Режим доступа: http://grebennikon.ru
12. ЭБС издательства «ЛАНЬ» [Электронный ресурс]. Режим доступа: http://e.lanbook.com

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4. Оценка качества освоения программы

Для итогового контроля усвоения данного курса учебным планом предусмотрен итоговый экзамен в форме тестирования. Итоговая аттестация проводится с использованием электронного обучения и дистанционных образовательных технологий. (далее – ДОТ и ЭО).

К итоговому аттестационному испытанию допускается лицо, успешно завершившее в полном объеме освоение программы дополнительного профессионального образования.

По итогам обучения проводится итоговый контроль знаний слушателей – экзамен по всей программе обучения (в форме тестирования) с применением тестового комплекса (тестовые задания, отражающие содержание каждой темы образовательной программы).

Итоговое аттестационное испытание проводится в соответствии с календарным учебным графиком, утвержденным в образовательной программе в дистанционном формате.

Условия проведения итогового экзамена в форме тестирования, представленной исполнителем (филиалом), члены комиссии фиксируют результаты в протоколе итогового аттестационного испытания в течение часа после завершения процедуры экзамена.

Члены комиссии в дистанционном фиксируют результаты в протоколе итогового аттестационного испытания в течение рабочего дня после завершения процедуры экзамена.

Итоговые испытания проводятся с участием не менее двух третей ее состава. Решения итоговых аттестационных комиссий принимаются на закрытых заседаниях простым большинством голосов членов комиссий, участвующих в заседании. При равном числе голосов председатель комиссии обладает правом решающего голоса.

По результатам любого из видов итоговых испытаний, включенных в итоговую аттестацию, выставляются отметки по четырехбальной системе («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).

Все решения итоговых аттестационных комиссий оформляются протоколами.

Лицам, не проходившим итоговых аттестационных испытаний по уважительной причине (временная нетрудоспособность или в других исключительных случаях, документально подтвержденных), предоставляется возможность пройти итоговые аттестационные испытания без отчисления из Академии, но не позднее 6 месяцев, начиная с даты выдачи оправдательного документа, предъявленного данным слушателем. Решение о признании причины уважительной принимает директор филиала.

Лица, не прошедшие итоговую аттестацию по неуважительной причине или получившие по итоговой аттестации неудовлетворительные оценки, подлежат отчислению из Академии.

Лица, допущенные к итоговой аттестации, но не проходившие ее по причине отчисления из Академии по своей инициативе, и лица, отчисленные из Академии в связи с непрохождением итоговой аттестации, могут быть восстановлены в Академии для прохождения (повторного прохождения) итоговой аттестации в соответствии с установленным Академией порядком.

В случае необходимости оспорить результаты итогового аттестационного испытания, слушатель вправе обратиться в апелляционную комиссию в соответствии с установленным Академией порядком. Апелляция подается слушателем в день объявления результатов итогового аттестационного испытания или в течение следующего рабочего дня. Апелляционные комиссии утверждаются в филиале и действуют до завершения рассмотрения апелляций по результатам последнего аттестационного испытания.

Экзамен в форме тестирования. Программа экзамена.

Тестирование – система заданий (задания на выбор одного или нескольких правильных ответов), созданная для объективного, качественного и эффективного метода оценки уровня подготовленности слушателей по программе.

Экзамен в форме тестирования проводится в использованием возможностей информационно-образовательного Интернет - портала ВШГУ РАНХиГС. Компьютерное тестирование проводится с помощью инструментов, встроенных в системы дистанционного обучения, или с помощью отдельных инструментов. Процесс

тестирования автоматизирован, осуществляется автоматическая обработка результатов тестирования, процедура оценивания в соответствии с установленным Академией порядком.

Тестирование проводится по месту нахождения слушателя.

Критерии оценки успеваемости слушателя на итоговой аттестации

Слушатель на итоговом аттестационном испытании получает для подготовки ответа 30 вопросов (тестов) из нижеприведенного перечня

Критерии оценки	Показатели
Оценка «отлично»	Слушатель ответил на 90% - 100 % и более тестовых вопросов
Оценка «хорошо»	Слушатель ответил на 80% - 89 % тестовых вопросов
Оценка «удовлетворительно»	Слушатель ответил на 70% - 79 % тестовых вопросов
Оценка «неудовлетворительно»	Слушатель ответил менее 70 % тестовых вопросов

Инструкция по прохождению тестирования

1. Общие положения

Тестирование состоит из вопросов с **закрытыми вариантами ответов** (выбор из предложенных). В вопросах может быть **один или несколько правильных ответов**. Внимательно читайте формулировку каждого задания. На выполнение всех заданий отводится **120 минут (2 часа)**. Результат определяется автоматически на основе выбранных вами ответов.

2. Порядок работы с тестом

До начала:

Убедитесь, что у вас есть стабильное интернет-соединение и устройство в заряженном состоянии. Подготовьте рабочее место, исключите отвлекающие факторы. Имейте под рукой черновик (бумажный или цифровой) для заметок и расчетов.

В процессе:

1. **Внимательно читайте каждый вопрос и все варианты ответов** до конца. Не торопитесь.
2. Обращайте особое внимание на формулировки:
   - «Выберите **правильный** ответ» – чаще всего подразумевает один вариант.
   - «Выберите **все правильные** ответы», «Какие из утверждений верны?», «Отметьте **верные** варианты» – подразумевают несколько правильных ответов.
3. Если вопрос вызывает затруднение:
   - Используйте **функцию «Отметить на потом»** (если она есть в интерфейсе теста).
   - Сделайте пометку в черновике с номером вопроса и переходите к следующему.
   - Не задерживайтесь на одном вопросе слишком долго.
4. Распределите время:
   - **Рекомендуется:** 100-110 минут на первичное решение всех вопросов, 10-20 минут – на проверку и возврат к отмеченным заданиям.
   - Контролируйте оставшееся время.

Оценочные средства
по дополнительной профессиональной программе
повышения квалификации

1. Что в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» понимается под информацией?

1) Конфиденциальные документированные сведения, зафиксированные на материальном носителе
2) Объективно отражающие действительность данные, полученные в результате информационных процессов
3) **Сведения (сообщения, данные) независимо от формы их представления**
4) Любые сведения, за исключением составляющих государственную тайну, представленные в форме, позволяющей их автоматизированную обработку

2. Какой федеральный закон регулирует обработку персональных данных?

1) Федеральный закон от 27.07.2006 № 149-ФЗ
2) Федеральный закон от 29.07.2004 № 98-ФЗ
3) **Федеральный закон от 27.07.2006 № 152-ФЗ**
4) Федеральный закон от 26.07.2017 № 187-ФЗ

3. Кто, согласно Федеральному закону «О персональных данных», может выступать в роли оператора персональных данных?

1) **Государственный или муниципальный орган, юридическое или физическое лицо, осуществляющий обработку персональных данных, а также определяющий цели обработки, состав персональных данных и действия, совершаемые с персональными данными**
2) Специализированный субъект, обладающий исключительной лицензией на деятельность в области обработки конфиденциальной информации и реализующий технические меры защиты данных
3) Публично-правовое образование или коммерческая организация, осуществляющие сбор и накопление персональных данных граждан исключительно на основании судебного решения
4) Исключительно юридическое лицо независимо от организационно-правовой формы, вступающее в правоотношения с субъектом персональных данных на основании публичного договора

4. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на…

1) создание условий для свободного обмена информацией и максимальной прозрачности деятельности организаций
2) полное уничтожение информации после истечения установленного срока её хранения
3) полное исключение любых рисков и инцидентов, связанных с данными
4) **соблюдение конфиденциальности информации ограниченного доступа**

5. Что понимается под информационной безопасностью?

1) Комплекс программно-технических средств, устанавливаемых на серверах и рабочих станциях для обнаружения и нейтрализации вредоносного программного обеспечения и сетевых атак
2) **Совокупность мер по защите данных от несанкционированного доступа, изменений, уничтожения или потери**

3) Совокупность правил разграничения доступа к документам и базам данных, устанавливаемая локальными нормативными актами организации-оператора
4) Исключительно совокупность организационных и технических мероприятий, направленных на предотвращение утечки конфиденциальной информации по техническим каналам связи

6. Какой орган государственной власти Российской Федерации наделен статусом уполномоченного органа по защите прав субъектов персональных данных и реализует функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства?
1) Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России)
2) Федеральная служба безопасности Российской Федерации (ФСБ России),
3) Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
4) Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

7. Своевременное обнаружение фактов несанкционированного доступа к информации и предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации относятся к обязанностям …
1) субъекта персональных данных
2) оператора информационных систем
3) Роскомнадзора
4) провайдера хостинга

8. Как называется единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также для реагирования на компьютерные инциденты в отношении информационных ресурсов Российской Федерации?
1) Единая система мониторинга и управления сетями связи общего пользования Российской Федерации
2) Национальный координационный центр по компьютерным инцидентам Российской Федерации
3) Система обеспечения выявления признаков компьютерных атак в единой сети электросвязи Российской Федерации
4) Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

9. Установление показателей критериев значимости объектов критической информационной инфраструктуры и порядка их категорирования относится к полномочиям …
1) Правительства Российской Федерации
2) Президента Российской Федерации
3) Министерства цифрового развития, связи и массовых коммуникаций
4) Роскомнадзора

10. Каким нормативным правовым актом устанавливаются состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных?
1) Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119
2) Приказ ФСТЭК России от 18 февраля 2013 г. № 21
3) Федеральный закон от 27 июля 2006 г. № 152-ФЗ

4) Приказ ФСТЭК России от 5 февраля 2010 г. № 58

11. В соответствии с требованиями Федерального закона «О персональных данных», какие из перечисленных ниже реквизитов являются обязательными для включения в письменное согласие субъекта персональных данных на обработку его персональных данных?

1) **Фамилия, имя, отчество субъекта; цель обработки; перечень персональных данных; наименование оператора; перечень действий с данными; срок действия согласия и способ его отзыва; подпись субъекта**
2) Только фамилия, имя, отчество и адрес субъекта; цель обработки; срок действия согласия; подпись субъекта
3) Фамилия, имя, отчество субъекта; наименование оператора; перечень персональных данных; перечень действий с данными; срок действия согласия; подпись субъекта
4) Фамилия, имя, отчество субъекта; цель обработки; перечень персональных данных; подпись субъекта

12. Какое определение соответствует понятию «биометрические персональные данные»?

1) Сведения об имущественном положении, доходах и расходах физического лица, используемые для оценки его платежеспособности при предоставлении кредитов и займов
2) Информация о национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья физического лица
3) **Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность**
4) Данные, позволяющие идентифицировать физическое лицо в информационно-телекоммуникационных сетях, включая сведения о сетевых идентификаторах (IP-адреса, cookie-файлы) и историю посещения веб-ресурсов

13. Информационная система - …

1) совокупность программно-аппаратных средств, объединенных в единую вычислительную сеть и предназначенных для автоматизации производственных процессов организации
2) **совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств**
3) комплекс организационно-распорядительной документации, регламентирующей порядок работы с информацией, и сотрудников, ответственных за ее обработку
4) техническое решение, включающее совокупность веб-сервисов и приложений, обеспечивающих удаленный доступ пользователей к информационным ресурсам через сеть Интернет

14. Какая классификация информации по видам предусмотрена Федеральным законом № 149 «Об информации, информационных технологиях и защите информации» в зависимости от порядка ее предоставления или распространения?

1) Информация делится на документированную и недокументированную, а также на электронную и аналоговую в зависимости от носителя и формы представления
2) Информация подразделяется на общедоступную, а также на информацию, отнесенную федеральным законом к сведениям, составляющим государственную тайну, коммерческую тайну, служебную тайну и иную охраняемую законом тайну
3) Информация классифицируется на массовую, рекламную, статистическую и персональные данные в зависимости от целевого назначения и содержания сведений

4) **Информация подразделяется на: свободно распространяемую; предоставляемую по соглашению лиц; подлежащую предоставлению или распространению в силу закона; информацию, распространение которой ограничивается или запрещается**

15. Что такое VPN как технология защиты информации при передаче данных в информационно-телекоммуникационных сетях?

1) Программа для скрытия IP-адреса пользователя при посещении веб-сайтов и обхода географических блокировок контента
2) **Технология, создающая зашифрованное соединение (туннель) между устройством пользователя и удаленным сервером, через которое направляется весь интернет-трафик, обеспечивая конфиденциальность и целостность передаваемых данных**
3) Аппаратное устройство, устанавливаемое на сервере организации и фильтрующее входящий и исходящий трафик по заданным правилам
4) Метод аутентификации пользователей при удаленном доступе к корпоративным ресурсам с использованием цифровых сертификатов и электронной подписи

16. Какой тип шифрования информации характеризуется использованием двух ключей — открытого для шифрования и закрытого для дешифрования?

1) Симметричное шифрование
2) **Асимметричное шифрование**
3) Поточное шифрование
4) Блочное шифрование

17. Что понимается под термином «фишинг» в области информационной безопасности и противодействия киберпреступности?

1) Метод автоматизированного подбора комбинаций логина и пароля для несанкционированного доступа к учетным записям пользователей
2) **Вид интернет-мошенничества, целью которого является получение несанкционированного доступа к конфиденциальным данным пользователей (логинам, паролям, данным банковских карт) путем использования поддельных электронных писем, веб-сайтов или сообщений, имитирующих официальные источники**
3) Физическое повреждение серверного оборудования или кабельной инфраструктуры с целью нарушения штатного режима функционирования информационной системы
4) Перехват и анализ радиосигнала беспроводных сетей Wi-Fi для последующего дешифрования трафика и получения несанкционированного доступа к передаваемым данным

18. В какой срок оператор обязан направить уведомление Роскомнадзор о своем намерении осуществлять обработку персональных данных в соответствии с требованиями Федерального закона «О персональных данных» (общий случай)?

1) **До начала обработки персональных данных**
2) В течение 30 рабочих дней с момента начала обработки персональных данных
3) Ежегодно, не позднее 1 февраля года, следующего за отчетным периодом
4) Уведомление не требуется для государственных и муниципальных органов, а также для бюджетных организаций

19. Сколько категорий значимости устанавливается для объектов критической информационной инфраструктуры Российской Федерации в соответствии с Федеральным

законом «О безопасности критической информационной инфраструктуры Российской Федерации»?

1) Одна категория
2) Две категории
3) **Три категории**
4) Четыре категории

20. Что означает принцип минимальных привилегий в контексте управления доступом и обеспечения информационной безопасности?

1) Ограничение доступа сотрудников к сети Интернет в рабочее время для предотвращения утечек информации
2) Запрет на наделение специалистов по информационной безопасности правами администратора информационной системы
3) Минимизация затрат на закупку оборудования и программного обеспечения для вновь принимаемых сотрудников
4) **Предоставление пользователю только тех прав доступа, которые необходимы для выполнения его непосредственных функциональных обязанностей**

21. Какой документ является итоговым и подтверждает успешное прохождение аттестации объекта информатизации на соответствие требованиям по защите информации?

1) Заключение по результатам аттестационных испытаний, подписанное экспертами органа по аттестации
2) **Аттестат соответствия требованиям по защите информации, выдаваемый органом по аттестации**
3) Технический паспорт на объект информатизации с отметкой органа по аттестации
4) Протокол аттестационных испытаний, утвержденный владельцем объекта информатизации

22. Что означает термин «нулевой день» в контексте уязвимостей программного обеспечения и информационной безопасности?

1) Уязвимость, которая существует в программном обеспечении более года без выпущенного обновления безопасности
2) Уязвимость, которая была обнаружена разработчиком в день выхода новой версии программного продукта
3) **Уязвимость, о которой разработчику программного обеспечения неизвестно и для которой на момент обнаружения не существует выпущенного официального обновления, устраняющего данную уязвимость**
4) Уязвимость, которая позволяет атакующему получить доступ к системе в течение первых 24 часов после ее обнаружения службой безопасности организации

23. Какое устройство относится к средствам инженерно-технической защиты информации, предназначенным для предотвращения утечки речевой информации по виброакустическому каналу?

1) Межсетевой экран, фильтрующий сетевой трафик на периметре информационной системы
2) Источник бесперебойного питания, обеспечивающий автономную работу оборудования при отключении электроэнергии
3) Система охранной сигнализации, реагирующая на несанкционированное проникновение в защищаемое помещение
4) **Виброизлучатель (вибропреобразователь), создающий маскирующие вибрационные помехи в элементах строительных конструкций**

24. Какая особенность характерна для технологии «песочницы», применяемой в современных антивирусных решениях и системах защиты информации?

1) Использование сигнатурного анализа для обнаружения известных вредоносных программ в режиме реального времени
2) **Изоляция подозрительного файла или программы в виртуальной среде с последующим поведенческим анализом для выявления скрытых и неизвестных угроз**
3) Шифрование всех входящих и исходящих данных для предотвращения их перехвата при передаче по каналам связи
4) Блокирование доступа к сетевым ресурсам на основе анализа IP-адресов и доменных имен отправителей

25. Какой основной недостаток присущ системам симметричного шифрования по сравнению с асимметричными криптосистемами?

1) Невозможность шифрования больших объемов данных из-за низкой скорости преобразования
2) **Необходимость предварительной передачи ключа шифрования сторонам коммуникации, что создает риски его перехвата при отсутствии защищенного канала**
3) Уязвимость к атакам на основе анализа побочных каналов (электромагнитное излучение, потребление энергии)
4) Обязательное использование только аппаратных средств реализации алгоритмов шифрования

26. Какие условия являются обязательными для получения организацией лицензии на проведение работ с использованием сведений, составляющих государственную тайну?

1) **Наличие в структуре организации подразделения по защите государственной тайны и специально подготовленных сотрудников, выполнение требований нормативных документов по обеспечению защиты государственной тайны, а также наличие сертифицированных средств защиты информации**
2) Наличие у руководителя организации допуска к государственной тайне по первой форме и положительной кредитной истории организации за последние три года
3) Прохождение организацией добровольной сертификации в системе сертификации средств защиты информации и наличие филиалов во всех федеральных округах Российской Федерации
4) Отсутствие у организации задолженности по налогам и сборам, наличие собственного отдельно стоящего здания и положительное заключение органов местного самоуправления

27. Что означает понятие «конфиденциальность информации» в контексте информационной безопасности?

1) **Состояние информации, при котором доступ к ней имеют только субъекты, имеющие на это право**
2) Свойство информации сохранять свою целостность и неизменность в процессе передачи по каналам связи
3) Возможность получения санкционированного доступа к информации при возникновении необходимости в любой момент времени
4) Совокупность методов и средств, обеспечивающих защиту информации от компьютерных вирусов и вредоносного программного обеспечения

28. С какой целью осуществляется процедура идентификации в системах контроля доступа и обеспечения информационной безопасности?

1) Для проверки подлинности предъявленных пользователем учетных данных (например, пароля или биометрического образца) путем сравнения с хранящимся эталоном
2) **Для присвоения пользователю уникального признака и его распознавания системой при последующих попытках доступа**
3) Для разграничения прав доступа пользователей к информационным ресурсам на основании их должностных обязанностей и уровня допуска
4) Для фиксации в журналах аудита всех действий, совершенных пользователем в системе, с целью последующего анализа и расследования инцидентов

29. Что представляет собой аутентификация как процесс обеспечения информационной безопасности?
1) Процедура присвоения пользователю уникального идентификатора, позволяющего системе отличать его от других пользователей
2) **Процесс проверки подлинности пользователя или системы, направленный на подтверждение их права доступа к определённым ресурсам или данным**
3) Процедура определения прав доступа пользователя к информационным ресурсам после его успешного входа в систему
4) Процесс фиксации всех действий пользователя в системе с целью последующего контроля и расследования инцидентов

30. Что представляет собой криптография в контексте информационной безопасности?
1) Технология шифрования информации, обеспечивающая ее конфиденциальность при передаче по каналам связи и хранении
2) Исключительно метод сокрытия факта существования информации с использованием стеганографических алгоритмов
3) **Комплекс методов и средств, обеспечивающих преобразование данных с целью скрытия их содержания, подтверждения подлинности, целостности и авторства**
4) Совокупность организационных мер по разграничению доступа к конфиденциальным документам в организации

31. Что представляет собой электронная подпись в соответствии с Федеральным законом «Об электронной подписи»?
1) Графическое изображение собственноручной подписи лица, отсканированное и вставленное в электронный документ для придания ему юридической силы
2) Специализированный USB-носитель (токен), выдаваемый удостоверяющим центром и являющийся материальным объектом, подтверждающим полномочия владельца
3) Криптографический алгоритм, предназначенный исключительно для шифрования электронных документов с целью обеспечения их конфиденциальности
4) **Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию**

32. Что представляет собой сертификат ключа проверки электронной подписи в соответствии с Федеральным законом «Об электронной подписи»?
1) Сам ключ электронной подписи (закрытый ключ), записанный на защищенный носитель и используемый для подписания электронных документов
2) Техническое устройство (токен), генерирующее пару ключей и обеспечивающее криптографические вычисления

3) **Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо его доверенным лицом и подтверждающий принадлежность ключа проверки электронной подписи ее владельцу**
4) Лицензия удостоверяющего центра на право осуществления деятельности по созданию и выдаче ключей электронных подписей

33. Что представляет собой распределенная атака типа DDoS-атака в контексте угроз информационной безопасности?
1) Атака, направленная на проникновение в защищенную сеть с целью кражи конфиденциальных данных путем подбора учетных записей
2) **Атака, осуществляемая одновременно с большого количества скомпрометированных устройств (бот-сети), целью которой является создание условий, при которых легитимные пользователи не могут получить доступ к ресурсу (веб-сайту, серверу, службе) из-за его перегрузки потоком ложных запросов**
3) Атака, заключающаяся во внедрении вредоносного кода в веб-приложения для получения контроля над сервером
4) Атака, направленная на перехват и модификацию трафика между двумя узлами сети без их ведома

34. Какие средства и способы обеспечения информационной безопасности являются наиболее эффективными при организации удаленного доступа к корпоративным ресурсам?
1) **Двухфакторная аутентификация, контроль действий пользователей в процессе сессии, проверка безопасности устройств, с которых осуществляется подключение, и проверка подлинности пользователя при входе в корпоративную сеть**
2) Использование только однофакторной аутентификации на основе сложных паролей без дополнительного контроля устройств и мониторинга действий
3) Применение исключительно антивирусного программного обеспечения на серверах без проверки безопасности клиентских устройств
4) Периодическое проведение инструктажей по информационной безопасности сотрудников без внедрения технических средств контроля доступа

35. Что представляет собой эксплойт в контексте информационной безопасности?
1) Метод шифрования данных при передаче по незащищенным каналам связи
2) Аппаратное средство защиты информации, устанавливаемое на периметре корпоративной сети
3) Политика безопасности, регламентирующая порядок смены паролей пользователями
4) **Программа, фрагмент кода или последовательность команд, разработанная для использования конкретной уязвимости в программном обеспечении с целью реализации несанкционированных действий**

36. Что представляет собой IP-адресация и какова ее основная функция в компьютерных сетях?
1) Физический (аппаратный) адрес, присваиваемый сетевому интерфейсу на заводе-изготовителе
2) **Уникальный числовой идентификатор (логический адрес), присваиваемый каждому устройству в компьютерной сети для обеспечения маршрутизации и идентификации узлов сети**

3) Имя устройства, используемое для удобного запоминания и доступа к ресурсам сети
4) Пароль для доступа к беспроводной сети, обеспечивающий аутентификацию пользователей

37. Какова основная функция системы доменных имен (DNS) в сетевой инфраструктуре?
1) Динамическое назначение IP-адресов устройствам при подключении к сети
2) **Преобразование (трансляция) удобочитаемых доменных имен (например, example.com) в числовые IP-адреса, необходимые для установления соединения**
3) Обеспечение шифрования трафика между клиентом и сервером
4) Фильтрация сетевого трафика на основе правил межсетевого экранирования

38. Какое назначение у протокола динамической конфигурации хоста (DHCP) в компьютерных сетях?
1) Разрешение доменных имен в IP-адреса
2) Обеспечение безопасного удаленного доступа к командной оболочке устройства
3) **Автоматическое назначение IP-адресов и других параметров сетевой конфигурации устройствам при их подключении к сети**
4) Передача гипертекстовых документов между веб-сервером и браузером клиента

39. Что представляет собой ransomware (программы-вымогатели) как класс вредоносного программного обеспечения?
1) Вредоносная программа, предназначенная для скрытого сбора и передачи конфиденциальной информации (паролей, данных банковских карт) злоумышленнику
2) **Тип вредоносного ПО, которое блокирует доступ к данным или системе (например, путем шифрования файлов) и требует выплаты выкупа за восстановление доступа**
3) Программа, отображающая навязчивую рекламу с целью получения дохода от рекламодателей
4) Вредоносное ПО, которое использует уязвимости системы для создания бэкдоров и обеспечения удаленного доступа злоумышленника к зараженному устройству

40. Что выступает основными источниками (причинами) возникновения программных уязвимостей в процессе разработки программного обеспечения?
1) Недостаточная квалификация пользователей и нарушение ими правил эксплуатации программного обеспечения
2) **Ошибки проектирования архитектуры, дефекты реализации (программирования), некорректные допущения о среде выполнения и недостаточная валидация входных данных**
3) Физическое старение оборудования и естественные сбои аппаратных компонентов
4) Целенаправленные действия злоумышленников по внедрению закладок на этапе эксплуатации

41. Что относится к средствам криптографической защиты информации (СКЗИ) согласно Положению ПКЗ-2005 (Приказ ФСБ России № 66)?
1) Программные средства шифрования, предназначенные для защиты информации при передаче по каналам связи
2) Аппаратные модули безопасности (HSM), сертифицированные ФСТЭК России

3) **Средства шифрования, средства имитозащиты, средства электронной цифровой подписи, средства кодирования, средства изготовления ключевых документов и ключевые документы**
4) Межсетевые экраны, системы обнаружения вторжений и антивирусное программное обеспечение

42. Какие требования предъявляются к размещению технических средств с установленными СКЗИ?
1) Размещение в любом помещении, имеющем розетку электропитания
2) Только в отдельно стоящих зданиях с охраной
3) Размещение исключительно в дата-центрах, имеющих уровень надежности Tier III и выше
4) **Размещение в помещениях, исключающих возможность бесконтрольного проникновения посторонних лиц, с минимизацией возможности неконтролируемого доступа непосредственно к средствам**

43. Какие действия являются первоочередными при обнаружении инцидента информационной безопасности для минимизации ущерба и обеспечения возможности последующего расследования?
1) Немедленное отключение питания всех задействованных серверов и рабочих станций для предотвращения дальнейшего распространения атаки
2) Уведомление правоохранительных органов до принятия каких-либо технических мер по сдерживанию инцидента
3) **Локализация инцидента путем отключения пораженных сегментов сети от коммуникаций и параллельный сбор информации (фиксация состояния систем, сохранение логов, создание криминалистических образов)**
4) Попытка самостоятельного удаления вредоносного программного обеспечения с использованием антивирусных утилит без предварительной фиксации состояния системы

44. Что представляют собой APT-атаки?
1) Массовые автоматизированные атаки с использованием стандартных вредоносных программ, направленные на случайных пользователей сети Интернет с целью получения быстрой финансовой выгоды
2) **Длительные, целенаправленные и скрытые кибератаки, при которых злоумышленники получают доступ к информационным системам и остаются незамеченными**
3) Атаки типа «отказ в обслуживании», реализуемые с использованием бот-сетей для перегрузки серверов целевой организации
4) Фишинговые атаки, направленные на массовый сбор учетных данных пользователей популярных интернет-сервисов

45. Двухфакторная аутентификация — это
1) **метод защиты данных, при котором для входа в систему применяется два независимых способа подтверждения личности**
2) метод защиты, удваивающий сложность пароля
3) обязательная повторная регистрация в системе для повышения безопасности
4) технология, требующая ввода логина и пароля два раза подряд

46. Какой принцип работы VLAN позволяет повысить производительность и безопасность локальной сети по сравнению с сетью, построенной на неуправляемых коммутаторах без сегментации?

1) VLAN обеспечивают шифрование всех передаваемых данных между коммутаторами, что исключает возможность перехвата трафика злоумышленниками
2) VLAN увеличивают пропускную способность каналов связи путем агрегации нескольких физических интерфейсов в один логический
3) **VLAN создают изолированные широковещательные домены на канальном уровне, ограничивая распространение широковещательного трафика только пределами виртуального сегмента, что снижает нагрузку на сетевое оборудование и предотвращает несанкционированный доступ между устройствами из разных VLAN**
4) VLAN позволяют подключать к одному порту коммутатора несколько устройств одновременно без использования дополнительного оборудования

47. Какие протоколы безопасности беспроводных сетей Wi-Fi считаются устаревшими и не подлежат применению в бюджетных организациях ввиду наличия критических уязвимостей, позволяющих осуществить взлом за несколько секунд или минут?

1) **WEP и WPA**
2) WPA2-Personal с AES (CCMP)
3) WPA3-Personal
4) WPA2-Enterprise

48. Почему использование открытых (незащищенных) Wi-Fi сетей в бюджетных организациях, например для организации гостевого доступа без аутентификации, создает критическую угрозу информационной безопасности?

1) Открытые сети имеют меньшую пропускную способность по сравнению с защищенными сетями
2) Открытые сети не позволяют подключить устройства, поддерживающие только протокол WPA3
3) **Открытые сети не обеспечивают шифрование трафика, что делает возможным перехват и анализ передаваемых данных с использованием инструментов сниффинга, а также реализацию атак типа MITM, включая ARP-спуфинг и подмену DNS**
4) Открытые сети требуют ежемесячной платы за использование, что увеличивает расходы бюджетной организации

49. Что представляет собой атака «злой близнец» и почему данная атака особенно опасна для бюджетных организаций, предоставляющих гостевой Wi-Fi доступ?

1) Атака, направленная на физическое уничтожение оборудования точки доступа путем воздействия электромагнитным импульсом
2) Атака, использующая уязвимости в прошивке бюджетных маршрутизаторов для внедрения вредоносного кода
3) Атака, при которой злоумышленник подбирает пароль к Wi-Fi сети методом перебора по словарю
4) **Атака, при которой злоумышленник создаёт поддельную точку доступа с именем, совпадающим с легитимной сетью**

50. Что представляет собой политика информационной безопасности организации как организационно-распорядительной документ?

1) Техническая инструкция по настройке межсетевых экранов и антивирусного программного обеспечения, разрабатываемая исключительно системными администраторами без согласования с руководством

2) **Внутренний нормативный документ, определяющий цели, задачи, принципы и направления деятельности организации в области обеспечения информационной безопасности, а также распределение ответственности и общие правила обработки защищаемой информации**
3) Ежегодный отчет о выявленных инцидентах информационной безопасности, направляемый в Роскомнадзор для подтверждения соответствия требованиям законодательства
4) Договор с внешней организацией на проведение аудита защищенности информационных систем и оказание услуг по мониторингу событий безопасности

5. ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ

Характеристика результатов освоения программы

В результате освоения программы у слушателя сформированы следующие компетенции:

Таблица

Компетенция (код, содержание)	Индикаторы
ПСК – 1.[6] Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД	- знать нормативные правовые акты в области связи, информатизации и защиты информации; - знать нормативные требования к составу и содержанию эксплуатационной документации СССЭ, а также средств и систем защиты СССЭ от НД; - знать номенклатура, функциональное назначение и основные характеристики средств и систем защиты СССЭ от НД - уметь проводить проверку комплектности СССЭ, средств и систем защиты СССЭ от НД; -уметь проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НД
ПСК – 2.[7] Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НД, средств для поиска признаков компьютерных атак в сетях электросвязи	- знать организационные меры по защите информации; -знать основные типы, основные характеристики средств измерений и контроля процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи; - понимать последовательность действий в целях изменения настроек СССЭ, а также средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи без прерывания процесса их функционирования проводить текущий контроль показателей и процесса функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи, предусмотренный регламентом их эксплуатации; - уметь выполнять предусмотренные в технической документации работы по изменению настроек СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи

[6] Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 536н (трудовая функция А/01.5)
[7] Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 536н (трудовая функция А/02.5)