ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

Автономная некоммерческая организация
высшего образования
«Центральный университет»

П Р И К А З

№ 0912.88 г. Москва «12» сентября 2024 г.

Об утверждении дополнительной профессиональной программы – программы повышения квалификации
«Обеспечение компьютерной безопасности (кибербезопасности)»

В целях организации образовательной деятельности по приоритетным направлениям

п р и к а з ы в а ю:

1. Утвердить дополнительную профессиональную программу – программу повышения квалификации «Обеспечение компьютерной безопасности (кибербезопасности)», реализуемую в АНО ВО «Центральный университет» (согласована с ФСТЭК России), 310 ак/ч, форма обучения – очно-заочная, в качестве приложения № 1 к настоящему приказу.
2. Контроль за исполнением настоящего приказа оставляю за собой.

Ректор Е.В. Ивашкевич

Приложение № 1
к приказу ректора
АНО ВО «Центральный университет»
от 12 сентября 2024 г. № 0912.88

Автономная некоммерческая организация высшего образования
«Центральный университет»

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Исполняющий обязанности начальника 1 управления ФСТЭК России	Ректор АНО ВО «Центральный университет»
_____ К.Сидорович	_____ Е.Ивашкевич
«10» 09 2024 г.	«12» сентября 2024 г.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

по направлению «Обеспечение компьютерной безопасности (кибербезопасности)»

Виды профессиональной деятельности:
организационно-управленческая, эксплуатационная

Трудоемкость обучения: 310 часов

Москва
2024

ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Общие положения

Настоящая программа повышения квалификации «Обеспечение компьютерной безопасности» (далее – программа повышения квалификации) разработана на основании Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», приказа Минобрнауки России от 19 октября 2020 г. № 1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности», приказа Минобрнауки России от 01 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» и приказа Минобрнауки России от 11 октября 2023 г. № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

Программа повышения квалификации в части электронного документооборота и защиты конфиденциальной информации (не содержащей сведения, составляющие государственную тайну, но защищаемой в соответствии с законодательством Российской Федерации), полностью соответствует требованиям «Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», утвержденного Постановлением Правительства Российской

Федерации от 16 апреля 2012 г. № 313 и «Положения о лицензировании деятельности по технической защите конфиденциальной информации», утвержденного Постановлением Правительства Российской Федерации от 03 февраля 2012 г. № 79.

Программа повышения квалификации реализуется в Автономной некоммерческой организации высшего образования «Центральный университет» (далее – АНО ВО «Центральный университет»).

Разработчики программы:

- Кадер Михаил Юрьевич, канд. техн. наук, Архитектор стратегических проектов
- Лукацкий Алексей Викторович, Бизнес-консультант по информационной безопасности
- Гадарь Дмитрий Александрович, вице-президент Тинькофф
- Кубышко Игорь Борисович, Руководитель управления реагирования на инциденты информационной безопасности
- Шипкова Нина Вячеславовна, руководитель направления Innostage
- Ингатов Олег Михайлович, магистр пед. образования

Программа повышения квалификации разработана в инициативном порядке.

1.2. Цель реализации программы

Программа повышения квалификации по информационной безопасности нацелена на развитие компетенций, критически необходимых для эффективного выполнения задач в сфере защиты информации. Она предоставляет участникам знания и навыки для приобретения новых профессиональных квалификаций, отвечающих текущим требованиям. Программа способствует удовлетворению образовательных и профессиональных потребностей участников, поддерживает их профессиональное развитие и обеспечивает соответствие их квалификаций меняющимся условиям в сфере информационной безопасности и требованиям современной социальной среды.

Программа является преемственной к основным образовательным программам высшего образования по:

– направлению подготовки 10.03.01 «Информационная безопасность», профиль подготовки «Безопасность автоматизированных систем», квалификация (степень) – бакалавр;

– специальности 10.05.03 «Информационная безопасность автоматизированных систем», квалификация – специалист по защите информации.

Программа ориентирована на профессиональный стандарт «Специалист по защите информации в автоматизированных системах», Приказ Минтруда России № 525н от 14 сентября 2022 г. https://mintrud.gov.ru/docs/mintrud/orders/244.

1.3. Категории обучающихся

Основными категориями обучающихся, на которых рассчитана программа повышения квалификации, являются руководители и специалисты структурных подразделений по защите информации и информационной безопасности, подразделений информационных технологий, подразделений, ответственных за организацию конфиденциального, в том числе электронного, документооборота органов государственной власти, органов местного самоуправления и организаций (предприятий) различных организационных форм и форм собственности.

1.4. Характеристика профессиональной деятельности обучившегося по программе повышения квалификации

а) Область профессиональной деятельности слушателя, прошедшего обучение по программе повышения квалификации, включает совокупность проблем, связанных с обеспечением защищённости объектов информатизации, в том числе информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере.

б) Объектами профессиональной деятельности являются:

- объекты информатизации, в том числе автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;
- технологии обеспечения информационной безопасности автоматизированных систем;

- системы управления информационной безопасностью автоматизированных систем.

в) Слушатель, успешно освоивший программу повышения квалификации, должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

эксплуатационная деятельность:

– установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности автоматизированных систем и иных объектов информатизации, с учетом установленных требований;

– участие в обследовании автоматизированных систем и иных объектов информатизации, их категорировании, классификации, определении требуемых уровней защищённости и аттестации по требованиям безопасности информации;

– администрирование систем информационной безопасности объектов;

– выполнение работ по защите информации.

организационно-управленческая деятельность:

– управление информационной безопасностью автоматизированных систем;

– контроль эффективности реализации политик информационной безопасности, реализованных в автоматизированных системах и иных объектах информатизации;

– участие в определении потребности в средствах защиты информации, контроль их поставки и правильной эксплуатации;

1.5. Планируемые результаты обучения

Обучение по программе повышения квалификации «Обеспечение компьютерной безопасности (кибербезопасности)» предполагает освоение соответствующих профессиональных компетенций:

- способность проводить анализ безопасности компьютерных систем;
- готовность проводить инструментальный мониторинг защищенности компьютерных систем и сетей;
- способность проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях.

Слушатель в результате освоения программы будет способен выполнять следующие должностные обязанности, приведённые в «Квалификационном справочнике должностей руководителей, специалистов и других служащих», утверждённом постановлением Министерства труда и социальной защиты Российской Федерации от 21 августа 1998 г. № 37 (в редакции Приказа Минтруда России от 12 февраля 2014 № 96).

Инженер по защите информации

Выполняет работу по проектированию и внедрению специальных технических и программно-математических средств защиты информации, обеспечению организационных и инженерно-технических мер защиты информационных систем, проводит исследования с целью нахождения и выбора наиболее целесообразных практических решений в пределах поставленной задачи. Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по техническим средствам и способам защиты информации. Участвует в рассмотрении проектов технических заданий, планов и графиков проведения работ по технической защите информации, в разработке необходимой технической документации. Составляет методики расчетов и программы экспериментальных исследований по технической защите информации, выполняет расчеты в соответствии с разработанными методиками и программами. Проводит сопоставительный анализ данных исследований и испытаний, изучает возможные источники и каналы утечки информации. Осуществляет разработку технического обеспечения системы защиты информации, техническое обслуживание средств защиты информации, принимает участие в составлении рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации, в написании и оформлении разделов научно-технических отчетов. Составляет информационные обзоры по технической защите информации. Выполняет оперативные задания, связанные с обеспечением контроля технических средств и механизмов системы защиты информации, участвует в проведении проверок учреждений, организаций и предприятий по выполнению требований нормативно-технической документации по защите информации, в подготовке отзывов и заключений на нормативно-методические материалы и техническую документацию. Готовит предложения по заключению соглашений

и договоров с другими учреждениями, организациями и предприятиями, предоставляющими услуги в области технических средств защиты информации, составляет заявки на необходимые материалы, оборудование, приборы. Участвует в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности. Проводит контрольные проверки работоспособности и эффективности действующих систем и технических средств защиты информации, составляет и оформляет акты контрольных проверок, анализирует результаты проверок и разрабатывает предложения по совершенствованию и повышению эффективности принимаемых мер. Изучает и обобщает опыт работы других учреждений, организаций и предприятий по использованию технических средств и способов защиты информации с целью повышения эффективности и совершенствования работ по ее защите и сохранению государственной тайны. Выполняет работы в установленные сроки на высоком научно-техническом уровне, соблюдая требования инструкций по режиму проведения работ.

Специалист по защите информации

Выполняет сложные работы, связанные с обеспечением комплексной защиты информации на основе разработанных программ и методик, соблюдения государственной тайны. Проводит сбор и анализ материалов учреждений, организаций и предприятий отрасли с целью выработки и принятия решений и мер по обеспечению защиты информации и эффективному использованию средств автоматического контроля, обнаружения возможных каналов утечки сведений, составляющих государственную, военную, служебную и коммерческую тайну. Анализирует существующие методы и средства, применяемые для контроля и защиты информации, и разрабатывает предложения по их совершенствованию и повышению эффективности этой защиты. Участвует в обследовании объектов защиты, их аттестации и категорировании. Разрабатывает и подготавливает к утверждению проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. Организует разработку и своевременное представление предложений для включения в соответствующие разделы

перспективных и текущих планов работ и программ мер по контролю и защите информации. Дает отзывы и заключения на проекты вновь строящихся и реконструируемых зданий и сооружений и другие разработки по вопросам обеспечения защиты информации. Участвует в рассмотрении технических заданий на выполнение эскизных, технических и рабочих проектов, обеспечивает их соответствие действующим нормативным и методическим документам, а также в разработке новых принципиальных схем аппаратуры контроля, средств автоматизации контроля, моделей и систем защиты информации, оценке технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений. Определяет потребность в технических средствах защиты и контроля, составляет заявки на их приобретение с необходимыми обоснованиями и расчетами к ним, контролирует их поставку и использование. Осуществляет проверку выполнения требований межотраслевых и отраслевых нормативных документов по защите информации.

Слушатель, освоивший программу повышения квалификации, должен ***знать:***

– место и роль информационной безопасности в системе национальной безопасности Российской Федерации;

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России (документы ведомства-заказчика программы) в данной области;

– правовые основы организации защиты государственной тайны и конфиденциальной информации;

– методики оценки и разработки моделей угроз информационной безопасности;

– правовые нормы и стандарты по лицензированию в области обеспечения защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, и сертификации средств защиты информации;

– систему организации комплексной защиты информации ограниченного доступа в системе, включая защиту персональных данных;

– технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;

– методы и способы несанкционированного доступа (НСД) к информации, способы и средства защиты от НСД к информации на объектах информатизации;

– методы и способы защиты информации с использованием СКЗИ;

– принципы и методы управления системой обеспечения информационной безопасности в ведомстве (предприятии, организации);

– существующие криптографические алгоритмы, используемые для ЗИ, и принципы построения защищенного документооборота с использованием электронной подписи и виртуальных частных систем;

– принципы организации информационных систем в соответствии с требованиями по защите информации.

уметь:

– анализировать и оценивать угрозы информационной безопасности объекта;

– пользоваться нормативными документами по защите информации;

– разрабатывать концепции, политики и иные организационно-распорядительные документы, необходимые для эффективного функционирования комплексных систем информационной безопасности объектов информатизации в организации;

– разрабатывать документы, необходимые для аттестации объектов информатизации по требованиям безопасности информации;

– правильно эксплуатировать системы и средства, предназначенные для эффективного функционирования комплексной системы защиты информации в подразделениях организации;

– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;

владеть:

– профессиональной терминологией;

– навыками применения средств антивирусной защиты;

– навыками организации и обеспечения режима защиты информации;

– навыками эксплуатации технических средств по оценке защищённости информации;

– методами технической защиты информации;

– методами организации и управления деятельности;

– методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

1.6. Трудоёмкость программы

Нормативная трудоемкость обучения по данной программе – 310 часов, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

1.7. Форма и сроки обучения

Обучение по программе повышения квалификации осуществляется в очно-заочной (без отрыва от работы) форме, а также с использованием дистанционных образовательных технологий.

Срок обучения в очно-заочной форме составляет – 10 недель.

1.8. Режим занятий

На этапе очного обучения режим занятий составляет не более 8 академических часов в день, с перерывом на обед – не менее 45 минут.

На этапе обучения с применением дистанционных образовательных технологий режим занятий не должен превышать более 4 академических часов в день.

Для всех аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При любой форме обучения учебная нагрузка устанавливается не более 54 часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

2. ПРОГРАММА УЧЕБНОГО КУРСА

2.1. Учебный план программы повышения квалификации «Обеспечение компьютерной безопасности (кибербезопасности)»

Категория слушателей (требования к слушателям) – высшее образование.

Продолжительность обучения – 310 часов.

Форма обучения – очно-заочная без отрыва от работы.

№ п/п	Наименование блоков учебного курса	Всего, академ. час.	В том числе		Формы аттестации и контроля знаний
			лекции	практич. и лаборат. занятия	
1	Экспресс киберучения	28	8	20	ТЗ
2	Что вы знали и не знали о SOC	30	15	15	ТЗ
3	Базовое погружение в особенности осуществления атак	50	25	25	ТЗ
4	Глазами атакующего	41	16	25	ТЗ
5	Инструменты и продвинутые подходы специалистов по расследованию	47	22	25	ТЗ
6	Создание контента SOC	44	18	26	ТЗ
7	Введение в Threat Intelligence и threat hunting	35	15	20	ТЗ
8	Выпускная работа	25		25	КП
9	Итоговая аттестация	10			ЗП

ТЗ – тестовое задание

КП – курсовой проект

ЗП – защита проекта

2.2. Учебно-тематический план программы повышения квалификации «Обеспечение компьютерной безопасности (кибербезопасности)»

Блок	Академ. часов	Наименование блока	Темы блока	Академ. часов
Блок 1	28	Экспресс киберучения	Средства мониторинга для киберучений	4
			Совместный разбор тестового кейса	4
			Практические занятия	20
Блок 2	30	Что вы знали и не знали о SOC	Что такое SOC? Цели и функции.	1
			Виды и эволюция SOC-центров	1
			Люди – технологии – процессы. Почему этого уже недостаточно?	2
			Распределение ролей в SOC. Возможен ли и какой карьерный рост в SOC.	1
			Жизненный цикл инцидента ИБ	4
			Ключевые процессы SOC	4
			Технологические платформы SOC	2
			Практические занятия	15
Блок 3	50	Базовое погружение в особенности осуществления атак	Основы безопасности компьютерных сетей	6
			Основы безопасности операционных систем	3
			Основы безопасности Windows	4
			Основы безопасности Linux	4

			Основы безопасности веб-приложений	4
			Open source решения	4
			Практические занятия	25
Блок 4	41	Глазами атакующего	Веб-атаки	8
			Инфраструктурные атаки	8
			Практические занятия	25
Блок 5	47	Инструменты и продвинутые подходы специалистов по расследованию	Работа с инструментами	6
			Безопасность компьютерных сетей	4
			Безопасность Windows	4
			Безопасность Linux	4
			Безопасность веб-приложений	4
			Практические занятия	25
Блок 6	44	Создание контента SOC	Use Cases	8
			Playbooks	10
			Практические занятия	26
Блок 7	35	Введение в TI и TH	Работа с сервисами аналитики угроз (TI)	4
			Знакомство с платформами TI и TH	2
			Основы анализа и поиска угроз. Построение гипотез	6
			Создание продуктов аналитики	3
			Практические занятия	20

Блок 8	25	Выпускная работа	Курсовой проект	25
Блок 9	10	Итоговая аттестация	Защита проекта	10

2.3. Практические занятия программы повышения квалификации «Обеспечение компьютерной безопасности (кибербезопасности)»

Блок	Тематика практического занятия	Академ. часов
Блок 1	Совместный разбор тестового кейса на киберполигоне	20
Блок 2	Описание ключевых процессов в SOC. Аналитическая работа.	15
Блок 3	Базовое погружение в особенности осуществления атак. Анализ систем безопасности современных ОС.	25
Блок 4	Описание веб-атаки	25
Блок 5	Анализ инструментов и продвинутых подходов по расследованию инцидентов ИБ	25
Блок 6	Написание playbooks	26
Блок 7	Работа с сервисами аналитики угроз (TI)	20

2.4. Примерные вопросы контроля знаний

- **Блок 1: Экспресс киберучения**

1. Какие инструменты мониторинга наиболее эффективны при проведении киберучений и почему?
2. Опишите процесс разбора тестового кейса киберучения. Какие ключевые аспекты следует учитывать?
3. Предложите сценарий практического занятия, направленного на развитие навыков быстрого реагирования на инциденты информационной безопасности.

- **Блок 2: Что вы знали и не знали о SOC**

1. В чем заключаются основные функции и цели SOC?

2. Как происходила эволюция SOC-центров и чем современные SOC отличаются от своих предшественников?
3. Почему интеграция "Люди – технологии – процессы" уже не является достаточной для эффективной работы SOC? Что еще необходимо учитывать?
4. Каковы перспективы карьерного роста в SOC и какие роли в этом могут быть задействованы?
5. Опишите жизненный цикл инцидента информационной безопасности в контексте SOC.

- **Блок 3: Базовое погружение в особенности осуществления атак**

1. Каковы основы безопасности компьютерных сетей и почему они важны для понимания механизмов кибератак?
2. Объясните ключевые аспекты безопасности операционных систем, на примере Windows и Linux.
3. Какие наиболее распространенные уязвимости встречаются в веб-приложениях?
4. Какие open source решения существуют для повышения уровня безопасности, и как их можно интегрировать в существующую инфраструктуру?

- **Блок 4: Глазами атакующего**

1. Опишите основные типы веб-атак и как им противостоять.
2. Какие инфраструктурные атаки наиболее часто используются злоумышленниками и какие меры предотвращения могут быть эффективны?
3. Приведите пример практического задания, которое поможет освоить техники защиты от инфраструктурных атак.

-
- **Блок 5: Инструменты и продвинутые подходы специалистов по расследованию**

1. Опишите подходы к обеспечению безопасности веб-приложений, которые должен знать каждый специалист по расследованию.
2. Предложите сценарий практического занятия, который позволит участникам курса научиться использованию продвинутых инструментов для расследования киберинцидентов.

- **Блок 6: Создание контента SOC**

1. Что такое Use Cases в контексте SOC и какова их роль в обеспечении информационной безопасности?

2. Опишите процесс создания и применения Playbooks в рамках SOC. Какие преимущества это дает?
3. Какие навыки и знания необходимы для эффективного создания контента SOC, такого как Use Cases и Playbooks?
4. Предложите задание для практических занятий, направленное на разработку Use Case или Playbook для реагирования на типичный инцидент безопасности.

- **Блок 7: Введение в TI и TH**

1. Какие основные функции и задачи сервисов аналитики угроз (Threat Intelligence, TI)?
2. В чем различие между платформами TI и TH, и какова их роль в управлении кибербезопасностью?
3. Как строить гипотезы в анализе угроз и почему это важно для прогнозирования и предотвращения инцидентов безопасности?
4. Опишите процесс создания продуктов аналитики на основе данных TI и TH. Какие ключевые моменты следует учитывать?
5. Предложите сценарий практического занятия, целью которого является анализ угроз и построение эффективных гипотез на основе данных из сервисов TI.

2.5. Календарный учебный график

Блок	Наименование блока	Темы блока	Академ. часов	Учебные недели									
				1	2	3	4	5	6	7	8	9	10
Блок 1	Экспресс киберучения	Средства мониторинга для кибербучений	4	4									
		Совместный разбор тестового кейса	4	4									
		Практические занятия	20	20									
Блок 2	Что вы знали и не знали о SOC	Что такое SOC? Цели и функции.	1		1								
		Виды и эволюция SOC-центров	1		1								
		Люди – технологии – процессы. Почему этого уже недостаточно?	2		2								
		Распределение ролей в SOC. Возможен ли и какой карьерный рост в SOC.	1		1								
		Жизненный цикл инцидента ИБ	4		4								
		Ключевые процессы SOC	4		4								
		Технологические платформы SOC	1		1								
		Практические занятия	15		15								
Блок 3	Базовое погружение в особенности	Основы безопасности компьютерных сетей	6			6							
		Основы безопасности операционных систем	3			3							

	осуществления атак	Основы безопасности Windows	4			4							
		Основы безопасности Linux	4			4							
		Основы безопасности веб-приложений	4			4							
		Open source решения	4			4							
		Практические занятия	25			10	15						
Блок 4	Глазами атакующего	Веб-атаки	8				8						
		Инфраструктурные атаки	8				8						
		Практические занятия	25				5	20					
Блок 5	Инструменты и продвинутые подходы специалистов по расследованию	Работа с инструментами	6					6					
		Безопасность компьютерных сетей	4					4					
		Безопасность Windows	4					4					
		Безопасность Linux	4					4					
		Безопасность веб-приложений	4						4				
		Практические занятия	25						25				
Блок 6	Создание контента SOC	Use Cases	8						8				
		Playbooks	10							10			
		Практические занятия	26							26			
Блок 7	Введение в TI и TH	Работа с сервисами аналитики угроз (TI)	4								4		
		Знакомство с платформами TI и TH	2								2		

		Основы анализа и поиска угроз. Построение гипотез	6								6		
		Создание продуктов аналитики	3								3		
		Практические занятия	20								20		
Блок 8	Выпускная работа	Курсовой проект	25									25	
Блок 9	Итоговая аттестация	Защита проекта	10										10

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы

Лица, желающие повысить квалификацию, должны иметь высшее профильное техническое образование, возможно смежное с УГНПС 10.00.00. Информационная безопасность (Электроника, радиотехника и системы связи, Инфокоммуникационные технологии и системы связи, Информатика и вычислительная техника, Информационные системы и технологии, Радиотехника, Прикладная информатика).

Наличие указанного образования должно подтверждаться документом государственного или установленного образца.

Желательно иметь стаж работы (не менее 1 года), связанной с эксплуатацией автоматизированных информационных систем; установкой, настройкой и обслуживанием средств защиты информации; разработкой организационно-распорядительных документов, регламентирующих вопросы защиты информации и обеспечения информационной безопасности.

Желательно также иметь опыт работы и навыки по управлению сетевой инфраструктурой на основе ОС Microsoft Windows Server; понимание принципов работы сетей TCP/IP.

3.2. Требования к кадровым условиям реализации программы

Реализация программы обеспечивается штатными руководящими и научно-педагогическими работниками АНО ВО «Центральный университет». В отдельных случаях, по согласованию с заказчиками, в целях более эффективной реализации программы, привлекаются специалисты производителей (вендоров) и дистрибьюторов конкретных средств защиты информации. Привлечение осуществляется на основе гражданско-правового договора. Обязательным условием привлечения внештатных преподавателей является наличие тренерского сертификата (сертификата специалиста по изучаемому продукту) от производителя.

Научно-педагогические работники, осуществляющие преподавание данной программы, имеют образование, соответствующее профилю преподаваемой дисциплины (модуля), конкретный опыт реализации научно-

прикладных разработок и иной формы практической деятельности в области информационной безопасности.

3.3. Требования к материально-техническим условиям реализации программы

Классы, оборудованные современным мультимедийным оборудованием, включая проекторы, интерактивные доски, и системы аудио-видео связи. Это обеспечивает возможность демонстрации обучающего материала в высоком качестве и проведения интерактивных занятий.

Для проведения лекций, изучения учебного материала и сдачи работ специализированная онлайн платформа. Платформа предоставляет инструменты для организации и контроля выполнения заданий и тестов.

Специализированные полигоны для практических занятий в сфере информационных атак и защиты. Эти полигоны представляют собой защищенные симулированные среды, где обучающиеся могут безопасно осуществлять практику по отражению кибератак и разработке мер защиты информационных систем.

3.4. Учебно-методическое обеспечение программы

Учебно-методические материалы включают: учебные и учебно-методические пособия по рассматриваемым темам; рабочие тетради (презентации, используемые для проведения учебных занятий, распечатанные в формате pdf.) по всем темам, читаемым в рамках курса; практикумы по отдельным темам учебной программы; CD–диски с нормативно-методическими и организационно-распорядительными документами, необходимыми для развёртывания и правильной организации эксплуатации различных средств технической и криптографической защиты информации. В ходе практических занятий используется программное обеспечение и техническая документация программных, аппаратных и программно-аппаратных средств технической и криптографической защиты информации.

В случае поступления заявок от лиц с ограниченными возможностями здоровья, т.е. физических лиц, имеющих недостатки в физическом и (или) психологическом развитии, подтвержденные психолого-медико-педагогической комиссией и препятствующие получению образования без создания

специальных условий, в АНО ВО «Центральный университет» создаются условия, позволяющие вышеприведённым категориям граждан, освоить программу повышения квалификации:

– возможно использование специальных педагогических подходов и наиболее подходящих для этих лиц языков, методов, способов общения и условий, в максимальной степени способствующих получению образования определенного уровня и определенной направленности;

– проведение занятий в отдельных классах, группах;

– предоставление возможности проведения занятий с использованием дистанционных образовательных технологий и электронного обучения;

– выделение сотрудников АНО ВО «Центральный университет», сопровождающих лиц с ограниченными возможностями здоровья, при нахождении в учебном центре;

– частичное снижение учебной нагрузки с учётом состояния обучаемого;

– сокращение часов аудиторных занятий до приемлемого минимума;

– оборудование учебных классов лабораторным оборудованием, позволяющим пользоваться им в зависимости от возможностей лица с ограниченными возможностями;

– предоставление бесплатно специальных учебников и учебных пособий, иной учебной литературы, а также услуг сурдопереводчиков и тифлосурдопереводчиков;

– обеспечение подготовки педагогических работников, владеющих специальными педагогическими подходами и методами обучения обучающихся с ограниченными возможностями здоровья.

3.5. Требования к информационному и учебно-методическому обеспечению программы

В процессе реализации программы повышения квалификации используются действующие правовые, нормативные и методические документы в области обеспечения информационной безопасности, документы национальной системы стандартизации, организационно-распорядительные и нормативные документы ФСБ и ФСТЭК России, а также соответствующие учебно-методические пособия и иллюстративный материал (презентации).

Приказы ФСТЭК России и приказы других федеральных органов исполнительной власти

1. Приказ ФСБ и ФСТЭК России № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».
2. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты».
3. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений».
4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
6. Приказ ФСТЭК России от 12 января 2023 года № 3 «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по технической защите конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. № 134 и внесенных в него изменений».
7. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «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».
8. Приказ ФСТЭК России от 27 сентября 2013 г. № 119 «Об утверждении требований к средствам доверенной загрузки».
9. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239.
10. Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и

Перечень используемых учебно-методических, правовых, нормативных и методических документов в области информационной безопасности, используемых при подготовке и в ходе реализации программы повышения квалификации, по каждому блоку занятий:

Блок 1. Экспресс киберучения

Печатные Материалы:

- Краткие руководства по основам кибербезопасности.
- Чек-листы для быстрой оценки уровня безопасности.

Учебные Пособия:

- "Основы Кибербезопасности" – сборник статей и кейс-стади.

Профильная Литература:

- Журналы и статьи по актуальным темам в кибербезопасности.
- Нормативные Документы:
- Перечень актуальных законов и норм в области кибербезопасности.

Электронные Ресурсы:

- Доступ к специализированным онлайн-платформам и базам данных.

Блок 2. Что вы знали и не знали о SOC

Печатные Материалы:

- Брошюры о функциях и задачах SOC (Security Operations Center).
- Учебные Пособия:
- "SOC для начинающих" – введение в структуру и принципы работы SOC.

Профильная Литература:

- Книги и статьи об опыте работы ведущих SOC.

Нормативные Документы:

- Гайдлайны и стандарты для SOC.

Электронные Ресурсы:

- Интерактивные симуляции работы SOC.

Блок 3. Базовое погружение в особенности осуществления атак

Печатные Материалы:

- Инфографика типов атак и методов защиты.

Учебные Пособия:

- "Типы кибератак: полный гайд" – детальное руководство.

Профильная Литература:

- Кейс-стади о наиболее значимых кибератаках последних лет.

Нормативные Документы:

- Обзор законодательства в области киберпреступлений.

Электронные Ресурсы:

- Виртуальные лаборатории для изучения методов кибератак.

Блок 4. Глазами атакующего

Печатные Материалы:

- Раздаточные материалы по основным стратегиям и тактикам атакующих.

Учебные Пособия:

- "Мир глазами хакера" – анализ тактик и стратегий киберпреступников.

Профильная Литература:

- Биографии известных хакеров и анализ их методов.

Нормативные Документы:

- Исследования по психологии киберпреступников.

Электронные Ресурсы:

- Сценарии для ролевых игр с позиции атакующего.

Блок 5. Инструменты и продвинутые подходы специалистов по расследованию

Печатные Материалы:

- Обзоры современных инструментов киберразведки.

Учебные Пособия:

- "Расследование киберпреступлений: продвинутые методы".

Профильная Литература:

- Статьи экспертов по кибербезопасности о техниках расследования.

Нормативные Документы:

- Примеры реальных кейсов расследования киберпреступлений.

Электронные Ресурсы:

- Интерактивные кейс-стади и симуляции расследований.

Блок 6. Создание контента SOC

Печатные Материалы:

- Руководства по созданию эффективного контента для SOC.

Учебные Пособия:

- "Контент-стратегии для SOC" – методы и практики.

Профильная Литература:

- Исследования о визуализации данных в кибербезопасности.

Нормативные Документы:

- Гайдлайны по стандартам контента в области безопасности.

Электронные Ресурсы:

- Шаблоны и инструменты для создания контента SOC.

Блок 7. Введение в TI и TH

Печатные Материалы:

- Вводные материалы по Threat Intelligence (TI) и Threat Hunting (TH).

Учебные Пособия:

- "Основы TI и TH" – комплексное руководство.

Профильная Литература:

- Анализ современных тенденций в TI и TH.

Нормативные Документы:

- Стандарты и протоколы в области TI и TH.

Электронные Ресурсы:

- Доступ к базам данных и аналитическим инструментам TI и TH.

Основная литература:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. «Основы информационной безопасности»: Учеб. пособие. -М.: Горячая линия-Телеком, 2006.
2. Тихонов В.А., Райх В.В., «Информационная безопасность: концептуальные, правовые, организационные и технические аспекты». Учебное пособие. - М.: Гелиос АРВ, 2006.
3. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. – М.: ГелиосАРВ, 2005.
4. Шаньгин В.Ф. «Защита компьютерной информации». - М.: ДМК Пресс, 2008.
5. Курило А.П., Зефиров С.Л., Голованов В.Б. «Аудит информационной безопасности». - М.: Издательская группа «БДЦ-пресс», 2006.
6. Хорев А.А. Защита информации от утечки по техническим каналам: Учеб. пособие. -М.: МО РФ, 2006.
7. Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006.
8. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебник для вузов. Под ре. Зайцева А.П. и Шелупанова А.А. Гриф Министерства образования и науки РФ. – 7-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2012.

9. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: Учеб. пособие, М.: Издательский центр «Академия», 2009.
10. Курило А.П., Милославская Н.Г., Сенатров М.Ю., Толстой А.И. Серия «Вопросы управления информационной безопасностью. Книга 1-5». Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2012.
11. Шнайер Б. «Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си». - М: Триумф, 2002.
12. Полянская О. Ю., Горбатов В. С. «Инфраструктуры открытых ключей». – М.: Интернет-университет информационных технологий, Лаборатория Знаний, 2007 г.

Дополнительная литература

1. Конституция Российской Федерации, принята 12 декабря 1993 г.
2. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
3. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
4. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
8. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».
9. Федеральный закон от 27 декабря 2002 г. № 184 «О техническом регулировании».
10. Закон Российской Федерации от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
11. Закон Российской Федерации от 13 июня 1996 г. № 63-ФЗ «Уголовный кодекс Российской Федерации».
12. Федеральный закон от 10 декабря 1995 г. № 196-ФЗ «О безопасности дорожного движения».

13. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне».

14. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 2 июля 2021 г. № 400.

15. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

16. Указ Президента Российской Федерации от 12 мая 2008 г. № 724 «Вопросы системы и структуры федеральных органов исполнительной власти».

17. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

18. Указ Президента Российской Федерации от 1 ноября 2008 г. № 1576 «О совете при Президенте Российской Федерации по развитию информационного общества в Российской Федерации».

19. Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

20. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

21. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

22. Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, утвержденная распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р.

23. Постановление Правительства Российской Федерации от 23 ноября 2012 г. № 1213 «О требованиях к тахографам, категориях и видах оснащаемых ими транспортных средств, порядке оснащения транспортных средств тахографами, правилах их использования, обслуживания и контроля их работы».

24. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

25. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

26. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

27. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

28. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

29. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

30. Постановление Правительства Российской Федерации от 18 сентября 2012 г. № 940 «Об утверждении правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с федеральной службой безопасности российской федерации и федеральной службой по техническому и экспортному контролю».

31. Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности».

32. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных

(криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

33. Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

34. Постановление Правительства Российской Федерации от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

35. Постановление Правительства РФ от 28 ноября 2011 г. № 976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи».

36. Постановление Правительства РФ от 09 февраля 2012 г. № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи».

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

38. Постановление Правительства Российской Федерации от 28 февраля 1996 г. № 226 «О государственном учете и регистрации баз и банков данных».

39. Постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

Приказы ФСТЭК России и приказы других федеральных органов исполнительной власти

1. Приказ ФСБ и ФСТЭК России № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».
2. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты».
3. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений».
4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
6. Приказ ФСТЭК России от 12 января 2023 года № 3 «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по технической защите конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. № 134 и внесенных в него изменений».
7. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «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».
8. Приказ ФСТЭК России от 27 сентября 2013 г. № 119 «Об утверждении требований к средствам доверенной загрузки».
9. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239.
10. Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и

обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235.

11. Требования к межсетевым экранам, утвержденные приказом ФСТЭК России от 9 февраля 2016 г. № 9.

12. Приказ Минтранса России от 21 августа 2013 г. № 273 «Об утверждении Порядка оснащения транспортных средств тахографами».

13. Приказ Минкомсвязи России от 27 октября 2011 г. № 282 «Об утверждении Положения о Департаменте государственной политики в области создания и развития электронного правительства Министерства связи и массовых коммуникаций Российской Федерации».

14. Приказ Роскомнадзора от 15 марта 2013 г. № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

15. Приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

16. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных». Утверждены Руководителем Роскомнадзора 13 декабря 2013 г.

17. Приказ Минкомсвязи России от 29 сентября 2011 г. № 242 «Об утверждении порядка передачи реестров квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи в случае прекращения деятельности аккредитованного удостоверяющего центра».

18. Приказ Минкомсвязи России от 23 октября 2011 г. № 321 «Об утверждении Административного регламента предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по организации ведения единого государственного реестра сертификатов ключей подписей удостоверяющих центров, обеспечению доступа к нему и к реестру сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, физических лиц и организаций».

19. Приказ Минкомсвязи России от 27 октября 2011 г. № 282 «Об утверждении Положения о Департаменте государственной политики в области создания и развития электронного правительства Министерства связи и массовых коммуникаций Российской Федерации».
20. Приказ Минкомсвязи России от 5 ноября 2011 г. № 250 «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».
21. Приказ Минкомсвязи России от 23 ноября 2011 г. № 320 «Об аккредитации удостоверяющих центров».
22. Приказ Минкомсвязи России от 13 апреля 2012 г. № 180 «Об обеспечении осуществления Министерством связи и массовых коммуникаций Российской Федерации функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров».
23. Приказ Минтранса России от 15 января 2014 г. № 7 «Об утверждении Правил обеспечения безопасности перевозок пассажиров и грузов автомобильным транспортом и городским наземным электрическим транспортом и Перечня мероприятий по подготовке работников юридических лиц и индивидуальных предпринимателей, осуществляющих перевозки автомобильным транспортом и городским наземным электрическим транспортом, к безопасной работе и транспортных средств к безопасной эксплуатации».
24. Приказ Минтранса России от 13 февраля 2013 г. № 36 «Об утверждении требований к тахографам, устанавливаемым на транспортные средства, категорий и видов транспортных средств, оснащаемых тахографами, правил использования, обслуживания и контроля работы тахографов, установленных на транспортные средства».
25. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России. - М., 1995.
26. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России. - М., 2006.
27. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. - М., 2006.

28. ГОСТ Р ИСО/МЭК 15408-1-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России. - М., 2008.
29. ГОСТ Р ИСО/МЭК 15408-2-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России. - М., 2008.
30. ГОСТ Р ИСО/МЭК 15408-3-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России. - М., 2008.
31. ГОСТ Р ИСО/МЭК 27001-2006. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
32. ГОСТ Р ИСО/МЭК 27002-2012. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
33. ГОСТ Р 51583-2014. Защита информации. Порядок создания информационных систем в защищённом исполнении. Общие положения.
34. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.
35. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении, утвержденная приказом ФСТЭК России от 25 декабря 2020 г.
36. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». - М, 1992.
37. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». -М., 1992.
38. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России. - М., 2008.

39. «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021).

3.6. Требования к условиям проведения занятий

Полный учебный цикл включает лекционные, практические и контрольно-проверочные занятия.

Не менее 50% времени курса повышения квалификации уделяется изучению практических вопросов организации защиты информации и эксплуатации изучаемых средств защиты информации. При этом в ходе проведения очных аудиторных занятий не менее 70 % учебного времени уделяется изучению практического использования средств технической и криптографической защиты информации.

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации. Часть лекций излагается проблемным методом с привлечением слушателей для решения сформулированных преподавателем проблем. К чтению лекций приказом руководителя образовательного учреждения допускаются наиболее опытные преподаватели.

На практические (лабораторные) занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических занятий по применению программных, программно-аппаратных средств защиты информации при их обработке в автоматизированных информационных системах, проводится в компьютерном классе с предварительной установкой необходимого программного обеспечения в компьютерной сети. При проведении практических занятий отрабатываются задания, учитывающие специфику выполняемых функциональных обязанностей слушателями курсов по своему профессиональному предназначению, в том числе предусматриваются занятия с проведением деловых игр.

В процессе практического обучения особое внимание уделяется формированию и развитию у слушателей практических умений и навыков.

Для проведения практических занятий используются методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий.

На практических занятиях отводится время для проверки знаний и навыков слушателей по пройденному материалу и усвоению изучаемой темы.

Для предупреждения несчастных случаев при отработке практических заданий в начале занятий со слушателями обращается внимание на правила техники безопасности. Преподаватель в ходе занятий обязан строго контролировать соблюдение слушателями установленных правил техники безопасности. В ходе занятий преподаватель несёт личную ответственность за правильное использование оборудования, приборов и соблюдение мер техники безопасности слушателями.

В целях повышения эффективности учебного процесса широко используются средства вычислительной техники, интернет технологии, средства виртуализации, презентации, схемы, плакаты, макеты, реальные программно-аппаратные и программные средства, образцы установленных форм документов и другие наглядные пособия.

При проведении учебных занятий с применением дистанционных образовательных технологий, реализуемых с применением информационно-телекоммуникационных сетей при опосредованном взаимодействии обучающихся и педагогических работников, используется система дистанционного обучения (СДО).

Слушателям предоставляется удаленный доступ к СДО через Интернет непосредственно с рабочих мест обучающихся. При этом каждый обучающийся является зарегистрированным пользователем СДО и имеет данные, необходимые для авторизации на сервере СДО в течение всего срока обучения. Регистрация обучающихся сопровождается рассылкой письменных уведомлений на адреса электронной почты и содержит следующую информацию, необходимую для авторизации и обучения на сервере СДО: информация о факте регистрации в СДО; адрес СДО (URL) в Интернете; имя учетной записи (логин); пароль; ссылка для скачивания «Руководства пользователя» для работы в СДО.

Система дистанционного обучения обеспечивает: трехзвенную архитектуру, состоящую из клиентской части (доступ к которой обеспечивается с помощью Интернет-браузера (рекомендуемый – Chrome), сервера СДО, обеспечивающего обработку поступающих запросов от зарегистрированных пользователей, и сервера базы данных (хранилище содержания дистанционных обучающих программ, пользовательского интерфейса и статистических

данных); круглосуточный удаленный доступ к СДО в режиме реального времени через Интернет в течение всего срока обучения; обязательную процедуру регистрации в СДО всех обучающихся (заведение новых пользователей с присвоением индивидуальной учетной записи и пароля); конфиденциальность регистрационных данных, обеспечивающуюся посредством автоматически сгенерированных СДО случайным образом индивидуальных паролей и последующей анонимной отправкой их на адреса электронной почты обучающихся; обязательную процедуру авторизации при каждом новом сеансе обучения; возможность изменения личных регистрационных данных после первичной регистрации, включая изменение пароля для входа в СДО; отображение стартовой страницы СДО (страницы авторизации) и содержимого курса в окне Интернет-браузера; тестирование пользователей на предмет оценки полученных знаний; пошаговую оценку действий пользователя; подсчет времени обучения и количества набранных баллов; наличие упражнений и демонстраций, созданных на основе экранных снимков изучаемых программных интерфейсов, имитирующих работу изучаемых средств защиты в соответствии со сценарием, и отображающихся обучаемым при выполнении упражнения по определенному алгоритму; показ методических указаний к упражнениям и демонстрациям с пошаговой инструкцией и подсказками; сбор и хранение статистики пошаговых действий обучаемых в СДО; сбор и хранение статистики в процессе тестирования и выполнения практических упражнений; возможность отображения и просмотра статистических данных по каждому вопросу тестового задания и пошаговым действиям, выполненным в процессе прохождения практических упражнений.

3.7. Порядок внесения изменений в программу повышения квалификации

Данная программа повышения квалификации подлежит переработке не реже, чем раз в три года, или при изменении нормативных правовых и методических документов ФСТЭК России и ФСБ России, регламентирующих принципиальные вопросы, связанные с тематикой модулей, рассматриваемой при реализации программы. Порядок внесения изменений в программу повышения квалификации и последующее согласование определяются действующими на момент переработки нормативными правовыми и иными документами Российской Федерации.

4. ФОРМЫ И КРИТЕРИИ АТТЕСТАЦИИ

4.1. Формы контроля и фонды оценочных средств

Оценка качества освоения программы включает текущую, промежуточную и итоговую аттестацию обучающихся.

Контрольно-проверочные занятия должны включать входной и текущий контроль, а также итоговую аттестацию обучающихся.

Входной контроль должен охватывать всех обучаемых и проводится в форме тестирования, проводимого с использованием СДО. Целью его является определение уровня знаний обучаемых для корректировки и адаптации учебного процесса под конкретные потребности обучаемых, с учётом уровня освоения учебного материала, изученного ими ранее в рамках получения базового образования или на курсах повышения квалификации.

Текущий контроль должен охватывать как можно большее число слушателей с обязательной оценкой их знаний, умений и навыков. Он должен стимулировать учебную работу слушателей и проводиться в форме, избранной преподавателем или предусмотренной рабочей программой.

Оценочные средства, включают типовые задания, выполняемые в ходе практических занятий и тесты, позволяющие оценить знания, умения и уровень приобретенных компетенций. В ходе тестирования используются современные способы и формы оценивания обучающихся, включая создание единой информационной среды с электронными формами контроля и оценки.

Основными критериями оценки усвоения слушателями учебного материала при проведении текущего контроля в ходе практических занятий являются: полнота ответов на поставленные вопросы; правильность выполнения действий при отработки практических вопросов эксплуатации изучаемых средств защиты информации; соответствие содержания и объёма выполненного задания поставленной задаче; правильность оформления; правильное форматирование отрабатываемых документов; правильность оформления ссылок на правовые, нормативные и методические документы; актуальность приведенных правовых, нормативных и методических документов; самостоятельность выполнения практических заданий.

При этом для каждого критерия оценки каждого практического занятия определяются весовые коэффициенты, позволяющие в определённом

конкретном случае получать наиболее объективные оценки выполненных слушателями заданий.

Программы текущего контроля и промежуточной аттестации максимально приближены к условиям (требованиям) их будущей профессиональной деятельности. С этой целью в качестве внешних экспертов при разработке привлекались специалисты Пенсионного фонда Российской Федерации.

Конкретные формы и процедуры входного и текущего контроля знаний по каждой теме разрабатываются учебным заведением самостоятельно и доводятся до сведения обучающихся в течение первого дня обучения.

Для проведения контрольно-проверочных занятий образовательным учреждением разработаны тестовые задания, включающие: организационно-методические указания по прохождению тестирования; вопросы для тестирования (не менее 20 вопросов для входного и промежуточных тестов и не менее 40 вопросов для итогового теста).

Тест включает в себя вопросы, направленные как на контроль знаний, так и на проверку полученных навыков работы. Во время тестирования запрещается пользоваться какой-либо литературой или заранее подготовленными записями.

При проведении тестирования с использованием единой информационной среды с электронными формами контроля и оценки у каждого слушателя есть три попытки на прохождение тестирования. Время на одну попытку - 40 минут. По окончанию попытки слушатель может видеть результаты теста и полученные баллы через две минуты после отправки результатов. При этом имеется возможность просмотра отчета, показывающего ошибки при прохождении теста. Оценка выставляется по последней попытке.

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей образовательной программы создаются фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить знания, умения и уровень приобретенных компетенций.

Фонды оценочных средств разрабатываются и утверждаются образовательным учреждением самостоятельно.

Освоение программы повышения квалификации специалистов завершается обязательной итоговой аттестацией.

4.2. Критерии оценки освоения программы повышения квалификации

Форма итоговой аттестации: Выпускные проектные работы оцениваются аттестационной комиссией на основе защиты проекта. Защита проекта включает в себя презентацию работы и ответы на вопросы комиссии.

Контрольно-измерительные материалы: Оценка проектной работы осуществляется по следующим критериям:

- Соответствие работы заявленной теме и целям проекта.
- Качество исследования и анализа.
- Оригинальность и инновационность подходов.
- Практическая значимость результатов.
- Качество презентации и защиты проекта.

Система оценок: Оценка за проектную работу выставляется по пятибалльной системе, где 1 является минимальной, а 5 - максимальной оценкой.

Балльно-рейтинговая система: Для более детальной оценки работы могут использоваться дополнительные баллы за отдельные элементы проекта (например, за исследовательскую работу, практическую часть, оформление и т.д.), которые затем переводятся в пятибалльную систему.

Критерии оценки:

- Отлично (5 баллов): Проект полностью соответствует всем вышеуказанным критериям и демонстрирует высокий уровень качества.
- Хорошо (4 балла): Проект соответствует большинству критериев, но имеются небольшие недочеты.
- Удовлетворительно (3 балла): Проект соответствует основным критериям, но имеются значительные недостатки.
- Почти удовлетворительно (2 балла): Проект имеет существенные недостатки в нескольких областях.
- Неудовлетворительно (1 балл): Проект не соответствует основным требованиям и целям.

Лицам, успешно освоившим соответствующую программу повышения квалификации и прошедшим итоговую аттестацию, выдаётся диплом о повышении квалификации. Диплом выдается на бланке, являющемся

защищенной от подделок полиграфической продукцией, образец которого самостоятельно установлен образовательным учреждением.

Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы повышения квалификации и (или) отчисленным из организации, выдается справка об обучении или о периоде обучения, по образцу, самостоятельно устанавливаемому организацией.