Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Кафедра информационной безопасности

Институт развития профессиональных
компетенций и квалификаций

ОБСУЖДЕНО И ОДОБРЕНО
на Ученом совете институтов и школ
дополнительного профессионального
образования
Протокол от 16.07.25 № 53

УТВЕРЖДАЮ
Проректор по дополнительному
профессиональному образованию
_____ Е.А. Диденко
«09» 07 2025 г.

ПРОГРАММА

повышения квалификации

«Администрирование средств защиты информации»

Москва – 2025

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«Администрирование средств защиты информации»
Общая характеристика программы

Цель программы – формирование и совершенствование у слушателей профессиональных компетенций, необходимых для обновления знаний, совершенствования навыков по различным аспектам профессиональной деятельности в области нормативно-правового обеспечения информационной безопасности, построения и модификации защищенных сетей по заданным схемам, организации межсетевого экранирования, защиты информации с использованием операционных систем специального назначения, контроля коммуникаций и предотвращения утечек.

Наименование профессиональных стандартов, квалификационных справочников, используемых при разработке ДПП:

Профессиональный стандарт 06.033 «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в процессе обучения:

- способность проводить техническое обслуживание систем защиты информации автоматизированных систем;
- способность проводить диагностику систем защиты информации автоматизированных систем;
- способность администрировать системы защиты информации автоматизированных систем;
- способность управлять защитой информации в автоматизированных системах.

Планируемые результаты обучения по программе

По итогам освоения программы слушатели должны:

Знать:

- типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях;
- базовую конфигурацию системы защиты информации автоматизированной системы;

- особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах;
- типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- нормативные и правовые акты в области защиты информации;
- национальные, межгосударственные и международные стандарты в области защиты информации;
- программно-аппаратные средства защиты информации автоматизированных систем;
- принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам.

Уметь:

- конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией;
- обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации;
- создавать, удалять и изменять учетные записи пользователей автоматизированной системы;
- устранять нарушения правил разграничения доступа;
- осуществлять контроль обеспечения уровня защищенности в автоматизированных системах.

Владеть:

- навыками, связанными с проверкой работоспособности системы защиты информации автоматизированной системы;
- технологией контроля соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации;
- технологией контроля стабильности характеристик системы защиты информации автоматизированной системы;
- навыками оценки защищенности автоматизированных систем с помощью типовых программных средств;
- технологией установки обновлений программного обеспечения автоматизированной системы;
- проведением занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне.

Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Кафедра информационной безопасности

Институт развития профессиональных
компетенций и квалификаций

ОБСУЖДЕНО И ОДОБРЕНО
на Ученом совете институтов и школ
дополнительного профессионального
образования
Протокол от 15.07.25 № 53

УТВЕРЖДАЮ
Проректор по дополнительному
профессиональному образованию
Е.А. Диденко
«15» 07 2025 г.

УЧЕБНЫЙ ПЛАН
программы повышения квалификации
«Администрирование средств защиты информации»

Требования к уровню образования слушателей	лица, имеющие среднее профессиональное и (или) высшее образование
Категория слушателей	работники, занимающиеся вопросами организации защиты информации
Срок обучения	152 часа
Форма обучения	очная (с применением дистанционных образовательных технологий и электронного обучения)
Режим занятий	8 часов в день

№ № п/п	Название модуля	Всего часов трудоемкости	В том числе				Форма контроля
			Контактная работа			Самостоятельная работа	
			Всего часов	из них			
				Лекции	Практические занятия		
1	Тема 1. Основные положения нормативно-правовых документов в области технической защиты информации	**8**	**8**	**6***	**2***	-	-
2	Тема 2. Защита информации с использованием операционной системы специального назначения Astra Linux SE и Alt Linux	**20**	**20**	**4***	**16***	-	Тестирование
3	Тема 3. Безопасность компьютерных сетей	**16**	**16**	**6**	**10**	-	Тестирование
4	Тема 4. Системы обнаружения вторжений	**16**	**16**	**6***	**10***	-	Тестирование
5	Тема 5. Защита сетевого периметра с использованием межсетевого экрана	**12**	**12**	**6***	**6***	-	Тестирование
6	Тема 6. Развертывание и администрирование межсетевого экрана «Континент 4»	**16**	**16**	**4**	**12**	-	Тестирование
7	Тема 7. Развертывание и администрирование MaxPatrol SIEM	**20**	**20**	**4**	**16**	-	Тестирование
8	Тема 8. Ввод, настройка и эксплуатация DLP-систем InfoWatch Traffic Monitor и SearchInform	**20**	**20**	**4**	**16**	-	Тестирование
9	Тема 9. Настройка и эксплуатация технических средств защиты от несанкционированного доступа (АМДЗ Аккорд и Соболь, СЗИ JaCarta и RuToken)	**10**	**10**	**4**	**6**	-	-
10	Тема 10. Администрирование средств антивирусной защиты рабочих станций и серверов, в т.ч. с использованием виртуализации	**12**	**12**	**4**	**8**	-	Тестирование
11	**ВСЕГО**	**150**	**150**	**48**	**102**	-	
12	**Итоговая аттестация**	**2**	**2**	-	**2**	-	**Экзамен в форме тестирования**
13	**Общая трудоемкость программы**	**152**	**152**	**48**	**104**	-	

Разработчик программы:

Капинос Сергей Павлович, доцент Кафедры информационной безопасности Факультета информационных технологий и анализа больших данных Финансового университета.

В реализации программы принимают участие эксперты и специалисты органов государственного управления, преподаватели Финансового университета, приглашенные ведущие специалисты в профильной сфере.

Директор ИРПКК Т.А. Болтенко

* С применением дистанционных образовательных технологий и электронного обучения

Федеральное государственное бюджетное учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Кафедра информационной безопасности

Институт развития профессиональных
компетенций и квалификаций

Календарный учебный график

программы повышения квалификации
«Администрирование средств защиты информации»

Объем программы – 152 час.
Продолжительность обучения – 19 рабочих дней
Форма обучения – очно (с применением дистанционных образовательных технологий и электронного обучения)

№ п\п	Наименование дисциплин (модулей), тем	1 день	2 день	3 день	4 день	5 день	6 день	7 день	8 день	9 день	10 день	11 день	12 день	13 день	14 день	15 день	16 день	17 день	18 день	19 день	КР	СР	ПА	С	ИА	Всего
1.	Тема 1. Основные положения нормативно-правовых документов в области технической защиты информации	8																			8					8
2.	Тема 2. Защита информации с использованием операционных систем специального назначения Astra Linux SE и Alt Linux		8	8	4																20					20
3.	Тема 3. Безопасность компьютерных сетей				4	8	4														16					16
4.	Тема 4. Системы обнаружения вторжений						4	8	4												16					16
5.	Тема 5. Защита сетевого периметра с использованием межсетевого экрана								4	8											12					12
6.	Тема 6. Развертывание и администрирование межсетевого экрана «Континент 4»										8	8									16					16

7.	Тема 7. Развертывание и администрирование MaxPatrol SIEM												8	8	4						20					20
8.	Тема 8. Ввод, настройка и эксплуатация DLP-систем InfoWatch Traffic Monitor и SearchInform														4	8	8				20					20
9.	Тема 9. Настройка и эксплуатация технических средств защиты от несанкционированного доступа (АМДЗ Аккорд и Соболь, ПНК JaCarta и RuToken)																	8	2		10					10
10.	Тема 10. Администрирование средств антивирусной защиты рабочих станций и серверов, в т.ч. с использованием виртуализации																		6	6	12					12
11.	Итоговая аттестация																			2	2					2
12.	Итого	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	152					152

Директор ИРПКК
« ___ » _____ 2025 г.

Т.А. Болтенко

Условные обозначения	
КР	контактная работа
СР	самостоятельная работа
ПА	промежуточная аттестация
С	стажировка
ИА	итоговая аттестация

Содержание тем

Тема 1. Основные положения нормативно-правовой документации в области технической защиты информации.

Обеспечение безопасности критической информационной инфраструктуры. Организация работы по категорированию объектов критической информационной инфраструктуры (далее – КИИ). Требования по обеспечению безопасности объектов КИИ. Варианты подключения объекта КИИ к системе к ГосСОПКА. Взаимодействие объекта КИИ с ГосСОПКА.

Обеспечение безопасности персональных данных (ПнД) при их обработке в информационной системе персональных данных (ИС ПнД). Комплексная защита ПнД в ИС ПнД. Организация работы с ПнД.

Тема 2. Защита информации с использованием операционных систем специального назначения Astra Linux SE и Alt Linux.

Архитектура операционных систем (ОС) GNU/Linux. Дистрибутивы Linux и Astra Linux. Особенности и преимущества Astra Linux. Краткое сравнение интерфейсов Astra | Alt Linux и Windows. Основные приёмы работы и настройки Astra | Alt Linux. Офисные приложения. Съемные носители и печать в Astra Linux. СЗИ в Astra | Alt Linux. Определение версий ОС и ядра.

Установка Astra | Alt Linux: изучение требований к компьютеру; подготовка к установке; установка ОС с локальных носителей (DVD, USB); установка ОС с ручной разметкой диска, настройка дополнительных параметров системы и выполнение необходимых действий после установки; установка обновлений систем; процесс загрузки ОС Linux.

Типы терминалов: аппаратный, виртуальный и псевдотерминал. Настройка терминалов. Утилита screen. Вход в систему и выход из системы, имена разных типов терминалов, настройка дисциплины линии, использование управляющих (Escape) последовательностей символов, работа с утилитой screen.

Основы работы в командной строке Astra | Alt Linux: структура строки; форматы записи параметров; работа с переменными; символы подстановки в именах файлов и командная подстановка; выполнение арифметических вычислений; отмена значений специальных символов; история команд; назначение псевдонимов; дополнение команд и имен переменных; выполнение команд, работа с переменными, составление шаблонов имен файлов, работа с историей команд, командная подстановка. Использование справочных ресурсов: отслеживание подсказок команд; использование помощи по встроенным в интерпретатор командам; работа со справочными

системами man и info; использование электронной справки Astra Linux и официальной документации; поиск ответов на вопросы на wiki.astralinux.ru.; навигация по справочной системе.

Работа с файлами в ОС Astra | Alt Linux: иерархия ФС; файлы, индексные дескрипторы, блоки данных; типы файлов; стандарт иерархии ФС (FHS); назначение основных каталогов; команды создания файлов и навигации по ФС; операции и поиск файлов. Использование Менеджера файлов и Midnight Commander для работы с файлами и каталогами. Навигация по ФС. Создание файлов разных типов, операции с файлами, поиск файлов.

Работа с текстовой информацией в ОС Astra | Alt Linux: перенаправление стандартных потоков в / из файла и между процессами; команды для просмотра текстовых файлов и команды-фильтры; регулярные выражения; потоковые фильтр grep и редакторы sed и awk; текстовый редактор vim и другие редакторы. Регулярные выражения и утилита grep, редактирование текстовых потоков с помощью sed, использование awk для составления командных строк.

Процессы в Linux: общие понятия о программах, процессах и потоках выполнения; жизненный цикл процесса; виды межпроцессного взаимодействия; настройка доступа к общим библиотекам; мониторинг процессов; управление приоритетом процесса; сигналы и управление заданиями. Мониторинг процессов и потоков в ОС, передача сигналов процессам, управление приоритетом и заданиями.

Управление учетными записями (УЗ) пользователей и групп: подготовка к созданию УЗ; изучение БД локальных УЗ; использование команд и графических утилит для создания, изменения и удаления УЗ; управление паролями; настройка окружения пользователя; управление аутентификацией и авторизацией с помощью PAM. Управление УЗ пользователей и групп, настройка параметров паролей, настройка окружения и рабочего стола пользователя, использование PAM-модулей.

Дискреционное управление доступом: индексный дескриптор файла и классы пользователей; стандартные права доступа и их интерпретация для файлов и каталогов; специальные биты защиты; символьная и числовая формы записи прав доступа; команды и инструменты для просмотра и изменения прав доступа; виды списков управления доступом к файлам и каталогам и утилиты для управления списками доступом; управление атрибутами файлами. Поиск файлов с заданными правами доступа. Изменение дискреционных прав доступа. Создание общих каталогов для пользователей с использованием общей группы и установкой бита sgid на каталог. Создание общих каталогов

для пользователей с использованием файловых списков доступа, использование атрибута файла a (append).

Мандатное управление доступом: уровни и категории конфиденциальности, мандатная целостность; состав метки безопасности; дополнительные мандатные атрибуты; определение уровней и категорий конфиденциальности; установка меток и дополнительных атрибутов безопасности на файлы и каталоги; установка допустимых мандатных уровней учетным записям пользователей; назначение PARSEC привилегий учетным записям пользователей. Организация совместной работы пользователей с файлами на разных уровнях конфиденциальности.

Архивация и сжатие данных: сжатие файлов; архивация файлов с учетом меток безопасности; синхронизация каталогов и файлов rsync; клонирование дисков. Использование команд dd, tar и утилиты rsync при работе с файлами с установленными метками безопасности.

Тема 3. Безопасность компьютерных сетей.

Краткое введение в безопасность компьютерных сетей (КС): Типовая IP-сеть. Уровни информационной инфраструктуры КС. Концепция глубокоэшелонированной защиты. Угрозы, уязвимости, атаки и варианты классификации. Обзор механизмов защиты КС. Базовые принципы сетевого взаимодействия. Архитектура TCP/IP. Краткая характеристика основного стека протоколов.

Безопасность физического и канального уровней: Сетевые анализаторы и «снифферы». Методы их обнаружения. Уязвимости сетевого оборудования. Проблемы аутентификации на основе MAC-адресов. Особенности работы механизма разрешения MAC-адресов в различных ОС. Проблемы безопасности протокола разрешения адресов ARP, варианты атак. ARP Spoofing. Меры защиты от атак на протокол ARP, утилита arpwatch. Обнаружение сетевых анализаторов с помощью протокола ARP, утилита Cain. Стандарт 802.1x и безопасность на уровне порта: Протокол EAP. Этапы построения сетевой инфраструктуры, удовлетворяющей требованиям стандарта 802.1x.

Безопасность сетевого уровня модели OSI: Протоколы IP и ICMP. Address Spoofing и его использование. Атаки с использованием протокола ICMP. Уязвимости механизма фрагментации.

Безопасность транспортного уровня модели OSI: Протоколы TCP и UDP. Распределённые DoS-атаки и меры защиты от них. DoS-умножение. Сканирование портов, утилита nmap. Атаки SYNFlood и LAND. Подмена

участника TCP-соединения. Разрыв TCP-соединения с помощью протокола ICMP.

Защита трафика на прикладном уровне: Протоколы SSL/TLS, SSH. Теория и практика атак «человек посередине».

Общие проблемы безопасности служб прикладного уровня: Уязвимости протокола DHCP. Обнаружение ложного DHCP-сервера. Изучение механизма DNS Spoofing.

Проблемы безопасности протокола IPv6: Краткое описание протокола. Проблемы безопасности. Итоговые рекомендации.

Виртуальные частные сети (VPN): Определение, разновидности, реализация технологии. Топологии. Схемы использования технологии. Краткие сведения об IPsec. Протоколы L2TP и PPTP. Сертифицированные решения для построения VPN.

Защита периметра сети: межсетевые экраны и их разновидности. Пакетные фильтры, технология StatefulInspection. Пакетный фильтр iptables на базе ОС Linux. Посредники и системы анализа содержимого. Изучение базовых возможностей межсетевого экрана Checkpoint NGX. Защита от атаки Address Spoofing.

Анализ защищённости корпоративной сети как превентивный механизм защиты: Классификация сканеров безопасности. Принципы анализа защищённости на сетевом уровне. Возможности и варианты использования сетевых сканеров безопасности. Работа с программой Internet Scanner.

Обнаружение сетевых атак: архитектура и классификация систем обнаружения. Анализ сигнатур. Виды сигнатур. Примеры систем обнаружения атак. Система обнаружения атак Snort.

Honeynet (сеть-приманка): Принципы организации. Классификация, практические реализации. Утилита honeyd, проект HoneyNet. Сценарии использования сетей-приманок. Риски, связанные с их использованием.

Тема 4. Системы обнаружений вторжений (IDS).

Необходимость технологии обнаружения атак. Обнаружение атак как механизм защиты. Терминология. События безопасности и уязвимости. Атаки. Модель традиционной и распределенной атаки. Этапы и средства реализации атак. Классификация атак. БД атак и уязвимостей. Инциденты. Архитектура систем обнаружений вторжений (СОВ).

Источники данных для СОВ. Принципы работы и варианты подключения сетевых СОВ. Скрытый режим работы сетевой СОВ. Обнаружение атак на уровне отдельного узла. Network Flow Data как дополнительный источник данных.

Признаки атак: повтор определенных событий; неправильные команды; использование уязвимостей; несоответствующие параметры сетевого трафика; несоответствие стандартам; непредвиденные атрибуты.

Методы обнаружения атак. Обнаружение аномалий и злоупотреблений. Анализ протоколов. Построение профиля поведения.

Механизмы реагирования. Варианты оповещений. Регистрация. Блокировка. Особенности использования СПА (систем противодействия атакам).

Специализированные СОВ. Особенности защиты беспроводных сетей. Защита от атак на СУБД и Web-приложения.

Взаимодействие с другими средствами защиты. Обнаружение атак и другие защитные механизмы. Корреляция.

Анализ результатов работы СОВ. Управление инцидентами.

Тема 5. Защита сетевого периметра с использованием межсетевого экрана.

Угрозы, связанные с периметром сети: Периметр корпоративной сети, понятие точки периметра. Угрозы, связанные с периметром сети. Составляющие защиты периметра.

Терминология: Основные термины и определения. Типы межсетевых экранов (МЭ). Расположение МЭ в корпоративной сети. Понятие демилитаризованной зоны.

Пакетные фильтры: Критерии фильтрации. Правила фильтрации. Реализация пакетных фильтров. Особенности фильтрации различных типов трафика. Недостатки пакетных фильтров.

Пакетный фильтр на базе ОС Linux: Архитектура и схема работы. Управление правилами фильтрации с помощью утилиты iptables.

Пакетный фильтр на базе ОС Windows: Служба RKAS. Программа управления службой RRAS.

Трансляция адресов: Типы трансляции. Реализация трансляции адресов в ОС Linux и Windows.

Технология Stateful Inspection: Принципы работы Stateful Inspection. Механизм определения состояния в iptables.

Посредники (proxy): Шлюзы уровня соединения. Классические и прозрачные посредники. Протокол SOCKS. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации.

Анализ содержимого: Контроль HTTP-трафика и электронной почты. Варианты решений. Системы анализа содержимого (контента).

Организация виртуальных частных сетей (VPN) на базе межсетевых экранов: Виды виртуальных частных сетей. МЭ как средство построения VPN.

Противодействие сетевым атакам при помощи МЭ: Механизмы реализации атак. Достоинства и недостатки МЭ как средств защиты. Проблема туннелирования. Возможности МЭ по обнаружению атак. Интеграция МЭ с другими средствами защиты.

Многофункциональные комплексы безопасности: Варианты классификации. Особенности реализации. Достоинства и недостатки различных решений по защите периметра.

Тема 6. Развёртывание и администрирование межсетевого экрана «Континент 4».

Назначение, состав, принципы функционирования и управление комплексом. Типовые аппаратные платформы и их производительность. Политика лицензирования. Порядок ввода комплекса в эксплуатацию.

Развертывание ЦУС Континент, рабочего места главного администратора и подчиненных узлов безопасности.

Управление узлами. Роли и назначение администраторов. Дистанционный доступ по протоколу SSH.

Настройка межсетевого экранирования: обработка трафика узлом безопасности; межсетевое экранирование; сетевые функции; виды объектов ЦУС; правила фильтрации и трансляции; установка политики.

Детектор атак: концепция управления СОВ; управление детектором атак в режимах Monitor | Inline; установка БРП и создание собственных сигнатур; формирование и установка политик СОВ. Инициализация, настройка и проверка функциональности детектора атак.

Построение VPN-туннеля; шифрование; топология; VPN с аппаратным ускорением шифрования; L2TP-туннель; VPN удаленного доступа.

Обеспечение отказоустойчивости комплекса: резервирование и восстановление конфигурации; аппаратное резервирование и восстановление УБ; резервирование БД ЦУС.

Мониторинг и аудит: общие сведения по системе мониторинга: инициализация, объекты мониторинга и типы информации, применение правил и шаблонов, просмотр сведений журналов.

Тема 7. Развёртывание и администрирование MaxPatrol SIEM.

Назначение SIEM-системы. Упрощенное внедрение системы. Компоненты системы, потоки данных. Установка системы, первичная настройка компонентов.

Asset and Vulnerability Management. Метрики CVSSv2, CVSSv3. Контекстные метрики. БДУ ФСТЭК РФ. Задачи, профили, активы: обнаружение узлов в сети, журналы агента; группы активов; аудит Windows и Linux; назначение контекстных метрик группам; топология.

Пользователи и роли, инфраструктуры.

Сбор и работа с событиями, PDQL и таксономия события. Сбор событий: WinEventLog, WMI Notification; File via SSH; группировка событий; сбор данных при помощи модуля FileMonitor SMB; работа с системой поиска событий при помощи языка запросов PDQL.

Корреляции и генераторы. Обзор системных правил корреляции. Сбор событий по протоколу syslog.

Инциденты и доставка уведомлений.

Работа с инцидентами и почтовыми уведомлениями: работа с автоматически созданным инцидентом; самостоятельное создание инцидента.

Статистика и отчеты. Построение отчетов.

Обзор документации. Журналы и решение проблем.

Решение проблем: файлы журналов; клиент к базе данных ElasticSearch.

Тема 8. Ввод, настройка и эксплуатация DLP-систем InfoWatch Traffic Monitor и SearchInform.

Определение криминальных тенденций. Профайлинг на службе ИБ.

Администрирование DLP-системы.

Практика применения DLP-системы. Advanced.

Тема 9. Настройка и эксплуатация технических средств защиты информации от несанкционированного доступа (АМДЗ Аккорд и Соболь, ПКН JaCarta и RuToken).

Настройка и эксплуатация указанных СЗИ от НСД.

Тема 10. Администрирование средств антивирусной защиты рабочих станций и серверов, в т.ч. и в среде виртуализации.

Антивирусная защита на рабочих станциях Windows. Антивирусная защита на серверах Windows и Linux. Антивирусная защита в среде виртуализации VMWare. Антивирусная защита почтовых систем.

Установка, настройка и эксплуатация антивирусного ПО: Kaspersky Endpoint Security and Management – базовый курс, масштабирование; Default Deny. Kaspersky Secure Mail Gateway. Dr.Web Enterprise Security Suite 12. Dr.Web для файловых серверов Windows.

Развертывание и администрирование Kaspersky Security Center для виртуальных сред по технологии легкого агента для платформы WebSphere (ESXi). Практическая работа с настройкой политик KSC (контроль устройств; веб-контроль; контроль приложений; адаптивный контроль аномалий; мониторинг файловых операций; анализ журналов; анализ поведения; защита от эксплоитов; предотвращение вторжений). Установка и настройка KSC на Linux-сервере. Установка и настройка продуктов Kaspersky для рабочих станций и серверов в Linux-системах (Astra, Alt). Загрузка сигнатур индикаторов компрометации (IOC) для детектирования средствами Kaspersky Endpoint Security. Проведение работ по установке обновлений системного и прикладного ПО при помощи Kaspersky Security Center.

Содержание практических занятий

№ темы	Наименование (содержание) темы, по которой предусмотрено занятие семинарского типа	Формы и методы проведения
1	Тема 1. Основные положения нормативно-правовых документов в области технической защиты информации	Выполнение практических заданий, работа на компьютере
2	Тема 2. Защита информации с использованием операционной системы специального назначения Astra Linux SE и Alt Linux	Выполнение практических заданий, работа на компьютере
3	Тема 3. Безопасность компьютерных сетей	Выполнение практических заданий, работа на компьютере
4	Тема 4. Системы обнаружения вторжений	Выполнение практических заданий, работа на компьютере
5	Тема 5. Защита сетевого периметра с использованием межсетевого экрана	Выполнение практических заданий, работа на компьютере
6	Тема 6. Развертывание и администрирование межсетевого экрана «Континент 4»	Выполнение практических заданий, работа на компьютере
7	Тема 7. Развертывание и администрирование MaxPatrol SIEM	Выполнение практических заданий, работа на компьютере
8	Тема 8. Ввод, настройка и эксплуатация DLP-систем InfoWatch Traffic Monitor и SearchInform	Выполнение практических заданий, работа на компьютере
9	Тема 9. Настройка и эксплуатация технических средств защиты от несанкционированного доступа (АМДЗ Аккорд и Соболь, СЗИ JaCarta и RuToken)	Выполнение практических заданий, работа на компьютере
10	Тема 10. Администрирование средств антивирусной защиты рабочих станций и серверов, в т.ч. с использованием виртуализации	Выполнение практических заданий, работа на компьютере

Список литературы:

Законодательные нормативные и правовые акты:

1. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

2. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

3. ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

4. ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

5. ГОСТ Р 53115-2008 Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства.

6. ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.

7. ГОСТ Р ИСО/МЭК 27034-1-2014 Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия.

8. ГОСТ Р ИСО/МЭК 27037-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.

9. ГОСТ Р ИСО/МЭК 29100-2013 Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности.

Основная литература:

10. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Юрайт, 2023. — 246 с. — (Высшее образование). — ЭБС Юрайт. — URL: https://urait.ru/bcode/512269 (дата обращения: 15.05.2025). - Текст : электронный.

11. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Юрайт, 2023. — 312 с. — ЭБС Юрайт. – URL:https://urait.ru/bcode/513300 (дата обращения: 15.05.2025). - Текст : электронный.

12. Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Юрайт, 2023 — 342 с. — (Высшее образование). — ЭБС Юрайт. - URL: https://urait.ru/bcode/515435 (дата обращения: 15.05.2025). — Текст : электронный.

13. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2021. — 327 с. — (Высшее образование). - ЭБС ZNANIUM.com. - URL: https://znanium.com/catalog/product/1189342 (дата обращения: 15.05.2025). — Текст : электронный.

Дополнительная литература:

14. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш. — 4-е изд., перераб. и доп. — Москва: РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). - ЭБС ZNANIUM.com. - URL: https://znanium.com/catalog/product/1861657 (дата обращения: 15.05.2025). – Текст : электронный.

15. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие для вузов / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов. – Москва : Горячая линия-Телеком, 2016. – 248 с. – ЭБС ZNANIUM.com. - URL: http://znanium.com/catalog/product/973806 (дата обращения 15.05.2025). - Текст : электронный.

16. Гамза, В. А. Безопасность банковской деятельности : учебник для вузов / В. А. Гамза, И. Б. Ткачук, И. М. Жилкин. — 5-е изд., перераб. и доп. — Москва : Юрайт, 2023. — 455 с.— ЭБС Юрайт. - URL: https://urait.ru/bcode/510990 (дата обращения: 15.05.2025). – Текст : электронный.

17. Кондрашов, Ю. Н. Язык SQL. Сборник ситуационных задач по дисциплине «Базы данных : учебно-практическое пособие / Ю. Н. Кондрашов. — Москва : Русайнс, 2021. — 125 с. — ЭБС BOOK.ru. - URL: https://book.ru/book/942020 (дата обращения: 15.05.2025). — Текст : электронный.

18. Стасышин, В. М. Базы данных: технологии доступа : учебное пособие для вузов / В. М. Стасышин, Т. Л. Стасышина. – 2-е изд., испр. и доп.

– Москва : Юрайт, 2023. – 164 с. – (Высшее образование). – ЭБС Юрайт. – URL: https://ezpro.fa.ru:2058/bcode/514252 (дата обращения: 15.05.2025). – Текст : электронный.

Интернет-ресурсы, информационно-справочные и поисковые системы:

19. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/
20. Электронно-библиотечная система BOOK.RU http://www.book.ru
21. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/
22. Электронно-библиотечная система Znanium http://www.znanium.com
23. Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru/
24. Электронно-библиотечная система издательства «Лань» https://e.lanbook.com/
25. Справочная правовая система КонсультантПлюс». [Электронный ресурс]. Режим доступа: http://www.consultant.ru/
26. Справочная правовая система «Гарант». [Электронный ресурс]. Режим доступа: http://www.garant.ru/iv/
27. Сайт компании Infotecs https://infotecs.ru/

Организационно-педагогические условия реализации программы повышения квалификации

1. Материально-технические условия, необходимые для осуществления образовательного процесса

Наименование специализированных учебных помещений	Вид занятий	Наименование оборудования, программного обеспечения
Учебный интерактивный класс	Все виды контактной работы	Мультимедийное оборудование, компьютеры. Компьютер, подключенный к сети Интернет, интернет-браузер. Прикладные программы для просмотра текстовых и видеоматериалов. ОС Astra Linux, ОС Alt Linux, МЭ Континент 4, MaxPatrol SIEM, DLP-система SearchInform, АМДЗ Аккорд, АМДЗ Соболь, Токен JaCarta, Токен RuToken, Kaspersky Endpoint Security, Kaspersky Security Center.

Материально-технические условия соответствуют действующим санитарным и противопожарным правилам и нормам.

Примечание. *В случае проведения учебных занятий с применением электронного обучения (ЭО) и дистанционных образовательных технологий (ДОТ) у слушателя должен быть персональный компьютер, оснащенный аудиоколонками, с доступом в сеть интернет и установленным видеоплеером, способным воспроизводить видеофайлы.*

2. Перечень информационных технологий и учебно-методическим условий, используемых при осуществлении образовательного процесса

Преподавателями используются компьютерные презентации, работу в чате, индивидуальное консультирование слушателей.

Условия для функционирования электронной информационно-образовательной среды

Электронные информационные ресурсы	Вид Занятий	Наименование оборудования, программного обеспечения
Система дистанционного обучения, система видеоконференцсвязи	Все виды контактной работы Итоговая аттестация	Компьютер, подключенный к сети Интернет; интернет-браузер; Прикладные программы для просмотра текстовых и видеоматериалов

3. Организация образовательного процесса

В образовательном процессе используются разнообразные формы работы со слушателями.

- лекция с мультимедийным сопровождением по наиболее сложным вопросам программы;
- практические занятия и самостоятельная работа с использованием современных технических средств обучения;
- кейс-стади – изучение конкретных ситуаций из практики (case-study), для выполнения данного вида заданий обучающимся должна быть представлена в письменной форме информация относительно реальной ситуации (профессиональной или жизненной) и поставлены конкретные задачи её изучения проблемы, обучающиеся анализируют различные аспекты проблемы и предлагают выработанные решения;
- тестирование метод оценки знаний, умений, навыков обучающихся и др.

Обучние проводится, в том числе с использованием ЭО и ДОТ, реализуемых посредством информационно-телекоммуникационных сетей при опосредованном взаимодействии слушателей и педагогических работников.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса, которые могут быть объединены в учебно-методический комплекс. Материалы учебно-методического комплекса доводятся до всех слушателей курса.

Итоговая аттестация проводится на образовательном портале Финансового университета посредством информационно-телекоммуникационных сетей.

4. Кадровое обеспечение образовательного процесса

Учебный процесс со слушателями обеспечивают квалифицированные сотрудники Финансового университета, а также приглашенные специалисты и действующие практики других организаций.

Описание системы оценки качества освоения программы

В систему оценки качества освоения программы «Администрирование средств защиты информации»

входят:

- текущий контроль;
- итоговая аттестация.

1. Текущий контроль успеваемости реализуется в ходе проведения практических занятий, обмена опытом работы, путем выполнения практических заданий, разбора конкретных ситуаций и тестирования.

2. Форма итоговой аттестации – экзамен в форме тестирования.

Примеры тестовых заданий для итоговой аттестации:

1. Злоумышленник с узла A провел атаку на узел B. IDS, установленная на узел C, обнаружила это и сообщила агенту MaxPatrol SIEM. Сообщение к агенту пришло с адреса D, сам агент имеет адрес E. Какой адрес указан в поле dst.ip?
2. У вас в локальной сети есть узел 172.31.234.123 и вы хотите построить отчет, в котором перечислены все соединения этого узла с внешним узлом 192.0.2.123 с распределением по времени. Ваши действия?
3. Перед вами стоит задача построить инвентаризационный отчет по активам. Как можно ограничить число активов, на основе информации о которых будет построен отчет?
4. Какой компонент применяется для хранения и обработки данных об активах информационной системы?
5. Какой компонент PT MaxPatrol SIEM предназначен для хранения журнальных данных?
6. Для чего предназначен компонент Update and Configuration Service (UCS)?
7. Расположите действия в порядке обработки системой MaxPatrol SIEM.
8. Перед вам нормализованное событие. Как узнать, какой модуль применялся для сбора события?
9. Что позволяет узнать запрос «http://storage:9200/_cat/indices?v»?
10. Какой журнал необходимо предоставить в техническую поддержку при сбое в пользовательском интерфейсе MaxPatrol SIEM?
11. Каково назначение поля reason в таксономии события?
12. Каково назначение поля tag в таксономии события?
13. Злоумышленник с узла A провел атаку на узел B. IDS, установленная на узел C, обнаружила это и сообщила агенту MaxPatrol SIEM. Сообщение к агенту пришло с адреса D, сам агент имеет адрес E. Какой адрес указан в поле event_src.ip?
14. Злоумышленник с узла A провел атаку на узел B. IDS, установленная на узел C, обнаружила это и сообщила агенту MaxPatrol SIEM. Сообщение к агенту пришло с адреса D, сам агент имеет адрес E. В каком поле таксономии будет храниться адрес E?

15. Чему должен быть равен параметр профиля «input_description_default_time_zone» при сборе журнальных сообщений с Chekpoint?
16. Принципы связи и обмен данными в локальной проводной сети.
17. Создание уровня доступа и распределения в сети Ethernet.
18. Планирование структуры локальной сети и подключение устройств.
19. IP-адреса и маски подсети.
20. Типы IP-адресов.
21. Получение IP-адресов и управление ими.
22. Взаимодействие клиентов и серверов.
23. Прикладные протоколы и сервисы.
24. Многоуровневая модель и протоколы.
25. Беспроводные локальные сети.
26. Обеспечение безопасности беспроводной локальной сети.
27. Настройка интегрированной точки доступа и беспроводного клиента.
28. Сетевые угрозы.
29. Методы атак.
30. Политика безопасности.
31. Использование межсетевых экранов.
32. Устранение проблем с сетями.
33. Общие проблемы, процесс и задачи устранения проблем.
34. Устранение неполадок и справочная служба.

Порядок проведения: тестирование проводится с личного компьютера, 50 тестовых вопросов, которые соответствуют разделам и темам, рассмотренным в рамках всей учебной программы, количество попыток – 3.

Для успешного прохождения итогового тестирования необходимо правильно ответить не менее чем на 35 тестовых вопросов в любой попытке.

Слушателям, которые успешно прошли итоговую аттестацию выдается удостоверение о повышении квалификации Финансового университета при Правительстве Российской Федерации.

Обсуждено и одобрено на заседании Научно-методического совета Института развития профессиональных компетенций и квалификаций, протокол № 33 от 03.07.2025.

Директор ИРПКК Т.А. Болтенко