Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

Институт цифровых технологий

УТВЕРЖДАЮ:
Первый проректор

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
00e605f899ce9c3b92f3e8601cfd84a822
Владелец: Огий Оксана Геннадьевна
Действителен: с 16.12.2025 по 11.03.2027

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
(программа повышения квалификации)
«КОМПЬЮТЕРНЫЕ СЕТИ И ПРИНЦИПЫ КИБЕРБЕЗОПАСНОСТИ»

Трудоемкость – *134* ч

Разработчик: *кафедра информационной безопасности*

Автор: *ст. преподаватель каф. ИБ Ильяшов А.Н.*

г. Калининград
2026

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная профессиональная программа (программа повышения квалификации), реализуется в соответствии с Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Приказом Минобрнауки России от 24.03.2025 № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», а также в соответствии с новой системой нормативных правовых актов по охране труда в Российской Федерации, введенных в силу с 01.01.2021 г.

Реализация программы повышения квалификации будет способствовать улучшению эффективности управления информационной безопасностью в организациях, снижению рисков возникновения киберинцидентов, в том числе на объектах критической информационной инфраструктуры. Программа предназначена для актуализации знаний кадров в области обеспечения информационной безопасности компьютерных сетей.

Цель:	повышение профессионального уровня специалистов в области построения, администрирования и защиты компьютерных сетей, обеспечения эффективного исполнения ими своих профессиональных обязанностей.
Задачи:	- повышение уровня профессиональных компетенций за счет актуализации знаний и умений в области компьютерных сетей и кибербезопасности; - совершенствование и углубление профессиональных компетенций, необходимых для выполнения трудовых функций, возложенных на специалиста в области построения, администрирования и защиты компьютерных сетей, специалиста по информационной безопасности в соответствии с действующими нормативными правовыми актами; - формирование практических навыков обнаружения, анализа и устранения сетевых угроз
Категория слушателей. (требования к квалификации слушателей):	лица, имеющие высшее образование или среднее профессиональное образование в области информационных технологий, информационной безопасности, занятые в должностях специалистов по информационной безопасности, системных администраторов, сетевых администраторов предприятий, учреждений, организаций
Срок освоения:	134 ч.
Режим занятий:	с отрывом от работы.
Форма обучения	очная, очно-заочная, применение электронного обучения и дистанционных образовательных технологий.

Планируемые результаты обучения. Компетентностный профиль программы.

Перечень компетенций, подлежащих совершенствованию, и (или) перечень новых компетенций, формирующихся в результате освоения.

В ходе освоения программы слушателем совершенствуются и углубляются профессиональные компетенции, необходимые для выполнения всех трудовых функций, возложенных на специалиста по информационной безопасности.

В результате освоения программы повышения квалификации обучающийся должен получить современные системные представления об обеспечении информационной безопасности на предприятии, основанные на действующем законодательстве Российской Федерации в этой области и передовом опыте работы; освоить новые стратегии обеспечения информационной и кибербезопасности на предприятии; расследованию и предупреждению киберинцидентов.

Программа обучения разработана на основании профессионального стандарта № 843 Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

ОТФ B.6: Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации.

ТФ (B/02.6) Администрирование систем защиты информации автоматизированных систем.

знания:	- программно-аппаратных средств защиты информации автоматизированных систем - методов контроля эффективности защиты информации от утечки по техническим каналам - принципов организации и структура систем защиты программного обеспечения автоматизированных систем - основных мер по защите информации в автоматизированных системах
умения:	- устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации - регистрировать события, связанные с защитой информации в автоматизированных системах - анализировать события, связанные с защитой информации в автоматизированных системах
трудовые действия:	- установка обновлений программного обеспечения автоматизированной системы - выполнение установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы - управление полномочиями доступа пользователей автоматизированной системы

ТФ (B/05.6) Мониторинг защищенности информации в автоматизированных системах

знания:
- основных угроз безопасности информации и модели нарушителя в автоматизированных системах
- программно-аппаратных средств обеспечения защиты информации автоматизированных систем
- методов защиты информации от утечки по техническим каналам
- нормативных правовых актов в области защиты информации
- руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации
- организационных мер по защите информации

умения:
- классифицировать и оценивать угрозы информационной безопасности
- анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах
- применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке
- контролировать события безопасности и действия пользователей автоматизированных систем

трудовые действия:
- выявление угроз безопасности информации в автоматизированных системах
- принятие мер защиты информации при выявлении новых угроз безопасности информации
- анализ недостатков в функционировании системы защиты информации автоматизированной системы
- устранение недостатков в функционировании системы защиты информации автоматизированной системы

Освоение слушателями программы повышения квалификации направлено на совершенствование следующих профессиональных компетенций:

ПК 1.2. Способность принимать участие в эксплуатации подсистем управления информационной безопасностью объекта защиты

ПК 1.3 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства

ПК 1.4 Способность администрировать подсистемы информационной безопасности объекта защиты

ПК 1.5 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

ПК 4.1. Способность принимать участие в формировании комплекса мер по обеспечению информационной безопасности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью

ПК 4.2. Способность организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта

защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации

ПК 4.3 Способность изучать и обобщать опыт работы различных учреждений, организаций и предприятий в области повышения эффективности защиты информации

ПК 4.5 Способность организовать технологический процесс защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

2. УЧЕБНЫЙ ПЛАН И КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

2.1 Учебный план

№ п/п	Наименование предметов, курсов, дисциплин (модулей)	Всего часов	В том числе			Форма контроля
			ЛК	ПЗ	СР	
1.	**Модуль 1: Основы построения компьютерных сетей**	**30**	12	12	6	Контроль на ПЗ
2.	**Модуль 2: Сетевые протоколы и технологии передачи данных**	**28**	10	12	6	Контроль на ПЗ
3.	**Модуль 3: Угрозы и уязвимости компьютерных сетей**	**32**	10	16	6	Контроль на ПЗ
4.	**Модуль 4: Средства и методы защиты компьютерных сетей**	**40**	8	24	8	Контроль на ПЗ
5.	**Итоговая аттестация**	**4**	-	-	4	Сертифицированное тестирование
	Итого часов	**134**	**40**	**64**	**30**	-

Примечание: при необходимости количество часов по отдельным модулям программы может быть изменено

2.2 Календарный учебный график

№ п/п	Наименование предметов, курсов, дисциплин (модулей)	Номер дня 1-й учебной недели с начала обучения[1]					Номер дня 2-й учебной недели с начала обучения					Номер дня 3-й учебной недели с начала обучения					
		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	6
		6 часов в день					8 часов в день					8 часов в день					
1	**Модуль 1.** Основы построения компьютерных сетей.	Т	Т	П	П	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х
2	**Модуль 2**. Сетевые протоколы и технологии передачи данных.	Х	Х	Х	Х	Т	Т/П	П	Х	Х	Х	Х	Х	Х	Х	Х	Х
3	**Модуль 3.** Угрозы и уязвимости компьютерных сетей.	Х	Х	Х	Х	Х	Х	Х	Т/П	Т/П	Т/П	П	Х	Х	Х	Х	Х
4	**Модуль 4.** Средства и методы защиты компьютерных сетей.	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Т	П	П	П	Х
5	**Итоговая аттестация**																И

[1]Даты обучения будут определены в расписании занятий при наборе группы на обучение

– учебная неделя; Т – теоретическое обучение; И –итоговая аттестация; × – нет недели

3. РАБОЧИЕ ПРОГРАММЫ ПРЕДМЕТОВ, КУРСОВ, ДИСЦИПЛИН (МОДУЛЕЙ) ПРОГРАММЫ

3.1 Рабочая программа дисциплины «Компьютерные сети и принципы кибербезопасности»

3.1.1 Пояснительная записка

Цель:	повышение теоретической и практической подготовки обучаемых в области построения, администрирования и защиты компьютерных сетей, а также приобретение умений и навыков работы с сетевым оборудованием, системами мониторинга и защиты сетевой инфраструктуры на примере использования средств, входящих в состав киберполигона Ampire.
В результате изучения слушатели должны:	
знать:	принципы работы сетевых протоколов и служб, методы и средства защиты компьютерных сетей, принципы работы систем обнаружения сетевых атак, методы мониторинга и анализа сетевой безопасности, основные компоненты компьютерных сетей и принципы их взаимодействия, сетевые протоколы всех уровней модели OSI и стека TCP/IP, методологию построения защищённых сетевых архитектур, подходы к выявлению и анализу компьютерных атак, средства и инструменты анализа сетевого трафика, принципы работы систем обнаружения и предотвращения вторжений, технологию использования и методику применения сенсоров ViPNet IDS; методы мониторинга и анализа событий и инцидентов информационной безопасности, технологию использования и методику применения системы анализа ViPNet TIAS, основы криптографии и механизмы аутентификации.
уметь:	проводить аудит сетевой инфраструктуры на предмет уязвимостей, обоснованно выбирать необходимые программные и программно-аппаратные средства защиты сетей, проводить мониторинг и анализ событий и инцидентов сетевой безопасности, организовывать поиск и использование оперативной информации о новых сетевых уязвимостях, разрабатывать предложения по совершенствованию политики информационной безопасности, применять инструментальные средства мониторинга и анализа сетевых событий, проводить диагностику и анализ инцидентов безопасности, настраивать системы защиты информации на базе современного программного и программно-аппаратного обеспечения, документировать результаты работ по обеспечению информационной безопасности, взаимодействовать с командой и руководством по вопросам обеспечения информационной безопасности.
владеть:	технологией мониторинга и анализа событий и инцидентов сетевой безопасности; методами и средствами выявления угроз безопасности компьютерных сетей; навыками по устранению уязвимостей в сетевой инфраструктуре; современными методами анализа сетевого трафика и выявления аномалий; навыками использования инструментов для мониторинга и анализа событий безопасности; приёмами работы с системами обнаружения и предотвращения вторжений.

3.1.2 Учебно-тематический план

№ п/п	Наименование предметов, курсов, дисциплин (модулей)	Всего часов	В том числе			Проверка знаний
			ЛК	ПЗ	СР	
1.	**Модуль 1: Основы построения компьютерных сетей**	**30**	12	12	6	Контроль на ПЗ
2.	**Модуль 2: Сетевые протоколы и технологии передачи данных**	**28**	10	12	6	Контроль на ПЗ
3.	**Модуль 3: Угрозы и уязвимости компьютерных сетей**	**32**	10	16	6	Контроль на ПЗ
4.	**Модуль 4: Средства и методы защиты компьютерных сетей**	**40**	8	24	8	Контроль на ПЗ
5.	**Итоговая аттестация**	**4**	-	-	4	Сертифицированное тестирование
	Итого часов	**134**	**40**	**64**	**30**	-

3.1.3 Содержание программы

МОДУЛЬ 1. ОСНОВЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Тема 1. Введение в компьютерные сети. Базовые понятия и определения

История развития компьютерных сетей. Основные понятия и определения. Классификация компьютерных сетей: локальные (LAN), городские (MAN), глобальные (WAN) сети. Топологии сетей: шина, звезда, кольцо, mesh. Клиент-серверная и одноранговая архитектура. Компоненты сетевой инфраструктуры.

Тема 2. Модель OSI и стек протоколов TCP/IP

Семиуровневая модель OSI: физический, канальный, сетевой, транспортный, сеансовый, представительский, прикладной уровни. Инкапсуляция данных. Модель TCP/IP и ее соответствие модели OSI. Сравнительный анализ моделей. Протоколы каждого уровня.

Тема 3. Физический и канальный уровни

Среды передачи данных: витая пара, оптоволокно, беспроводные среды. Стандарты Ethernet (IEEE 802.3).

MAC-адресация. Коммутаторы и их функции. Технология VLAN. Протокол STP/RSTP. ARP-протокол.

Тема 4. Сетевое оборудование

Концентраторы, коммутаторы, маршрутизаторы, межсетевые экраны. Принципы работы и назначение. Коммутация пакетов и кадров. Базовая настройка сетевого оборудования. Управление коммутаторами и маршрутизаторами.

Тема 5. Адресация в IP-сетях

IPv4-адресация: классы адресов, маски подсети, CIDR-нотация. Частные и публичные адреса. NAT и PAT.

IPv6-адресация: структура адреса, типы адресов. Планирование IP-адресации. Подсети и суперсети.

МОДУЛЬ 2. СЕТЕВЫЕ ПРОТОКОЛЫ И ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ

Тема 6. Протоколы транспортного уровня

TCP: установление соединения (three-way handshake), управление потоком, контроль ошибок, завершение соединения. UDP: дейтаграммная передача, области применения. Порты и сокеты. Сравнение TCP и UDP.

Тема 7. Протоколы маршрутизации

Статическая и динамическая маршрутизация. Классификация протоколов маршрутизации: IGP и EGP, distance-vector и link-state. RIP, OSPF, EIGRP, BGP. Административное расстояние и метрики. Таблицы маршрутизации.

Тема 8. Протоколы прикладного уровня

HTTP/HTTPS, FTP/SFTP, SMTP/POP3/IMAP, DNS, DHCP, Telnet/SSH, SNMP, NTP. Принципы работы и области применения. Анализ трафика прикладных протоколов.

Тема 9. Технологии виртуальных частных сетей (VPN)

VPN: концепция, виды (site-to-site, remote access). Туннельные протоколы: PPTP, L2TP, IPSec, SSL/TLS VPN. Шифрование и аутентификация в VPN. Настройка VPN-соединений.

Тема 10. Беспроводные сети

Стандарты Wi-Fi (IEEE 802.11a/b/g/n/ac/ax). Архитектура беспроводных сетей. Точки доступа, контроллеры WLAN. Частотные диапазоны и каналы. Роуминг. Технологии безопасности: WEP, WPA, WPA2, WPA3.

Тема 11. Качество обслуживания (QoS)

Необходимость QoS в современных сетях. Модели QoS: Best Effort, IntServ, DiffServ. Классификация и маркировка трафика. Управление очередями, полиция и шейпинг. Приоритизация голосового и видео трафика.

МОДУЛЬ 3. УГРОЗЫ И УЯЗВИМОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Тема 12. Основы информационной безопасности компьютерных сетей

Основные принципы информационной безопасности: конфиденциальность, целостность, доступность (CIA). Модель угроз и нарушителя. Классификация угроз безопасности сетей. Законодательство РФ в области защиты информации.

Тема 13. Сетевые атаки и методы их реализации

Разведка и сканирование сетей. Сниффинг трафика. Атаки на протоколы: ARP-spoofing, DNS-spoofing, IPspoofing. MITM-атаки. Атаки на уровне приложений.

Тема 14. Атаки типа «отказ в обслуживании»

DoS и DDoS атаки: SYN-flood, UDP-flood, ICMP-flood, HTTP-flood. Усиленные DDoS-атаки. Ботнеты. Методы обнаружения и противодействия DoS/DDoS атакам.

Тема 15. Уязвимости сетевых протоколов и служб

Уязвимости протоколов канального уровня: CAM-overflow, VLAN hopping, STP-атаки. Уязвимости маршрутизации. Уязвимости DNS, DHCP. Уязвимости беспроводных сетей. База данных уязвимостей (CVE, NVD).

Тема 16. Методы обнаружения и анализа уязвимостей

Сканирование сетей: Nmap, Masscan. Анализ трафика: Wireshark, tcpdump. Сканеры уязвимостей: Nessus, OpenVAS. Пентестинг сетевой инфраструктуры. Metasploit Framework. Составление отчетов о выявленных уязвимостях.

МОДУЛЬ 4. СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ

Тема 17. Политика безопасности компьютерных сетей

Разработка политики сетевой безопасности. Модели управления доступом. Сегментация сети и изоляция критичных ресурсов. Принцип наименьших привилегий. Аудит и мониторинг безопасности.

Тема 18. Межсетевые экраны (Firewall)

Типы межсетевых экранов: пакетные фильтры, stateful firewall, proxy firewall, NGFW. Правила фильтрации трафика. ACL (Access Control Lists). Демилитаризованная зона (DMZ). Настройка firewall на базе Linux (iptables, nftables) и аппаратных решений.

Тема 19. Системы обнаружения и предотвращения вторжений (IDS/IPS)

Классификация IDS/IPS: сетевые (NIDS/NIPS) и хостовые (HIDS/HIPS). Методы обнаружения: сигнатурный, аномальный, гибридный. Snort, Suricata. Настройка правил обнаружения. Управление ложными срабатываниями.

Тема 20. Системы управления событиями безопасности (SIEM)

Концепция SIEM. Сбор и корреляция событий безопасности. Анализ логов сетевого оборудования и систем защиты. Визуализация и оповещение. Расследование инцидентов. Примеры SIEM-систем: ViPNet TIAS, Splunk, ELK Stack, MaxPatrol SIEM.

Тема 21. Криптографические методы защиты

Симметричное и асимметричное шифрование. Алгоритмы шифрования: AES, RSA. Электронная подпись.

Сертификаты и инфраструктура открытых ключей (PKI). Протоколы защищенной передачи данных:

SSL/TLS, IPSec, SSH. Настройка защищенных каналов связи.

Тема 22. Защита беспроводных сетей

Угрозы безопасности Wi-Fi сетей. Защита на уровне точек доступа. Протоколы аутентификации: 802.1X, EAP. RADIUS-серверы. Безопасная конфигурация беспроводных сетей. Системы обнаружения несанкционированных точек доступа (Rogue AP Detection).

Практические занятия по защите сетей

Проектирование защищенной корпоративной сети. Настройка межсетевых экранов и IDS/IPS. Мониторинг сетевого трафика. Симуляция сетевых атак и отработка сценариев реагирования на инциденты. Анализ и устранение уязвимостей.

3.1.4 Промежуточная аттестация по программе

Промежуточная аттестация по курсу не предусмотрена. Проверка знаний слушателей проводится непосредственно в ходе проведения практических занятий. Основная цель контроля – получение обратной связи путем анализа хода формирования знаний и умений. По его результатам преподаватель при необходимости вносит корректировку в планы проведения занятий.

3.1.5 Обеспеченность образовательного процесса учебной литературой и информационными ресурсами

Материалы по программе размещаются на http://eios.klgtu.ru/mod ЭИОС КГТУ. Доступ к материалам осуществляется после регистрации на основании договора об оказании образовательных услуг по программе ДПП.

В ходе обучения могут использоваться следующие материалы:

1. Методические материалы для работы с программным комплексом обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire»
2. Кузьмин О.В., Чефранова А.О., Фефилов А.В. Безопасность КИИ. – М., 2020. – 326 с.
3. Руководство администратора. Программно-аппаратный комплекс ViPNet TIAS
4. Выписка из руководства администратора. Программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS NS
5. Методический документ/ Методика оценки угроз безопасности информации (утвержден ФСТЭК России 5.02.2021).
6. Документация на продукты ViPNet представлена в виде pdf-файлов на сайте https://infotecs.ru/downloads/documentacii/
7. Банк данных угроз безопасности информации (https://bdu.fstec.ru/)

8. Дополнительные материалы и учебно-методические комплексы на сайте:
https://infotecs-edu.ru/materials/
https://infotecs-edu.ru/kompleksy/
9. Куроуз Дж., Росс К. Компьютерные сети. 6-е издание. – СПб.: Питер, 2016.
10. Смирнов В.Л., Шестаков С.А. Информационная безопасность: защита и нападение. 3-е издание. – М.: ДМК Пресс, 2020.
11. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие. – М.: Горячая линия-Телеком, 2013.
12. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2003.
13. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е издание. – СПб.: Питер, 2012.
14. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 5-е издание. – СПб.: Питер, 2016.
15. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
16. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах».
17. Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014).
18. Профессиональный стандарт № 843 «Специалист по защите информации в автоматизированных системах» (утв. приказом Минтруда России от 14.09.2022 № 525н).
19. Платформа VulDB - база данных уязвимостей: https://vuldb.com/
20. Веб-интерфейс для данных об уязвимостях CVE: https://www.cvedetails.com/
21. Национальная база данных уязвимостей США: https://nvd.nist.gov/
22. База знаний о тактике и методах нарушителей MITRE ATT&CK: https://attack.mitre.org/
23. Документация Cisco по сетевым технологиям: https://www.cisco.com/c/en/us/tech/
24. Документация Snort IDS/IPS: https://www.snort.org/documents
25. Документация Suricata IDS/IPS: https://suricata.readthedocs.io/
26. Материалы и документация Wireshark: https://www.wireshark.org/docs/
27. Веб-интерфейс для данных об уязвимостях CVE https://www.cvedetails.com/
28. Поиск информации/ База знаний на www.opennet.ru https://www.opennet.ru/search.shtml
29. Материалы базовых сценариев (zip-архивы);
30. Презентации по сценариям киберучений.

4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

4.1 Материально-техническое обеспечение учебного процесса

В ходе освоения программы слушатели используют возможности интерактивной коммуникации со всеми участниками и заинтересованными сторонами образовательного процесса, ресурсы и информационные технологии посредством электронной информационной образовательной среды университета.

Перечень современных профессиональных баз данных и информационных справочных систем, к которым обучающимся по образовательной программе обеспечивается доступ (удаленный доступ) является ежегодно обновляемым приложением к рабочим программам дисциплин (рассматривается УМС и утверждается отдельно) и размещается на официальном сайте в разделе «Образовательные программы высшего образования университета» и в ЭИОС.

При дистанционном обучении преподавателю обеспечивается доступ к платформе проведения вебинаров в соответствии с расписанием. Технические и программные средства обеспечиваются слушателем самостоятельно.

Занятия проводятся в компьютерном классе ауд.363 ГУК:
– персональный компьютер с ОС Астра Линукс;
– проектор;
– программное обеспечение «AMPIRE»;
– доступ в сеть Интернет.

Оборудование:

- Персональные компьютеры (рабочие станции) – не менее 12 единиц
- Сетевое оборудование: управляемые коммутаторы, маршрутизаторы, точки доступа Wi-Fi
- Проектор и экран для демонстрации материалов
- Сервер виртуализации для развертывания лабораторных стендов

Программное обеспечение:

- Операционные системы: Windows, Linux (Ubuntu, CentOS, Kali Linux)
- Средства виртуализации: VirtualBox, VMware
- Программы анализа сетевого трафика: Wireshark, tcpdump
- Средства сканирования: Nmap, Nessus, OpenVAS
- Системы обнаружения вторжений: Snort, Suricata
- Средства тестирования на проникновение: Metasploit Framework
- Эмуляторы сетевого оборудования: GNS3, Cisco Packet Tracer
- Межсетевые экраны: iptables, pfSense

При всех формах реализации программы должны соблюдаться требования соответствующих СанПиН.

4.2 Организация образовательного процесса

Реализация программы осуществляется в соответствии с требованиями к организации образовательного процесса в университете, изложенными в локальных нормативных актах.

Приведенное выше распределение модулей и тем занятий по дням занятий может уточняться с учетом выбранной формы обучения (очной, очно-заочной, заочной с применением электронного обучения и дистанционных образовательных технологий).

Обучение осуществляется на образовательной площадке университета и носит непрерывный характер. Преподаватели консультируют слушателей как в очном режиме, так и в режиме онлайн.

Курс по программе повышения квалификации планируется к реализации в соответствии с расписанием курсов, утвержденным директором ИЦТ.

Продолжительность одного учебного дня составляет 8 академических часов. Один академический час составляет 40 минут. Через каждые два часа предусмотрены 15-минутные перерывы, продолжительность обеденного перерыва составляет 60 минут. Рабочая неделя составляет 30-40 часов. Курс 3 недели

Программа разработана на основе практико-ориентированного подхода. Её освоение позволит слушателям решать на современном уровне практические задачи, связанные с функциями по обеспечению требований по защите информации в своих организациях.

Особенности реализации программы:

1. **Модульная структура:** программа состоит из четырех взаимосвязанных модулей, последовательное изучение которых обеспечивает формирование системных знаний.
2. **Практическая направленность:** до 40% времени отводится на практические занятия, включая работу с реальным и виртуальным сетевым оборудованием.

3. **Лабораторные работы:** слушатели выполняют практические задания в специально подготовленной лабораторной среде, моделирующей реальные сетевые инфраструктуры.

4. **Кейсы и сценарии:** разбор реальных инцидентов информационной безопасности, симуляция атак и отработка сценариев реагирования.

4.3 Кадровое обеспечение

Требования к преподавателям, обеспечивающим реализацию программы (лекторам, ассистентам, лаборантам:

Реализация программы обеспечивается профессорско-преподавательским составом, отвечающим одному из следующих критериев:

– наличие ученой степени (ученого звания) по направлению читаемых дисциплин;

– наличие опыта практической работы не менее 3 лет по направлению дисциплины и опыта преподавательской работы не менее 2 лет.

К реализации программы привлекаются как штатные преподаватели университета, так и сторонние специалисты по договорам гражданско-правового характера.

4.4 Методические рекомендации по реализации программы

Для успешного овладения дисциплиной слушателям рекомендуется:

1. Принимать участие во всех лекционных и практических занятиях.
2. Все рассматриваемые на лекциях и практических занятиях вопросы фиксировать либо на бумажных, либо электронных носителях (вести конспект).
3. Обязательно выполнять все рекомендации по самостоятельной работе, получаемые на лекциях или практических занятиях.
4. В случае пропуска занятий восполнить пропущенные темы самостоятельно по материалам дисциплины.
5. Активно использовать лабораторное оборудование и программное обеспечение для закрепления теоретических знаний.
6. Самостоятельно изучать дополнительную литературу и документацию по сетевым технологиям и средствам защиты.

Методические указания по проведению практических занятий:

1. Перед началом практического занятия необходимо провести инструктаж по технике безопасности и правилам работы с оборудованием
2. Практические задания должны выполняться последовательно, с постепенным усложнением
3. Преподаватель должен демонстрировать выполнение типовых операций на примерах
4. Слушатели должны иметь возможность самостоятельно экспериментировать с конфигурациями в безопасной среде
5. По результатам каждого практического занятия слушатели должны оформить отчет с описанием выполненных действий, полученных результатов и выводов
6. Рекомендуется использовать технологии виртуализации для создания изолированных тестовых стендов.

5. ИТОГОВАЯ АТТЕСТАЦИЯ ПО ПРОГРАММЕ

Итоговая аттестация по программе проводится в форме тестирования. Тест включает 10 программированных вопросов. Аттестация будет считаться успешной при правильном ответе не менее чем на 8 вопросов.

Итоговая аттестация может быть реализована также в формате проведения киберучения по одному из сценариев, реализованных в ПАК «AMPIRE».

Лицам, успешно освоившим ДПП и прошедшим итоговую аттестацию, выдается документ о повышении квалификации, оформляемый на специальном бланке за подписью ректора университета.

ЛИСТ СОГЛАСОВАНИЯ

Дополнительная профессиональная программа (программа повышения квалификации) «**КОМПЬЮТЕРНЫЕ СЕТИ И ПРИНЦИПЫ КИБЕРБЕЗОПАСНОСТИ**» утверждена на заседании учебно-методической комиссии Института цифровых технологий.

Зам. директора Института
цифровых технологий по ДО и ПП  Е.В. Кривопускова