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:
096e64c14d2c5a4a542a3f05d72293e2
Владелец: **Огий Оксана Геннадьевна**
Действителен: **с 21.10.2024 по 14.01.2026**

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

(программа повышения квалификации)

«Обнаружение, анализ и устранение последствий компьютерных атак на базе программного комплекса «Ampire»

Трудоемкость – *140* ч

Разработчик: *кафедра информационной безопасности*

Автор: *ст. преподаватель каф. ИБ Подтопельный В.В.,*
ассистент каф. ИБ Ильяшов А.Н.

г. Калининград
2025

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная профессиональная программа (повышение квалификации) (далее - ДПП), реализуется в соответствии с Федеральным законом от 29.12.2012 г. № 273-ФЗ "Об образовании в Российской Федерации", Приказом Минобрнауки России от 01.07.2013 № 499 «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 и на объектах КИИ. Программа предназначена для актуализации знаний кадров в области обеспечения информационной безопасности.

Цель:	повышение профессионального уровня специалистов по информационной безопасности, обеспечения эффективного исполнения ими своих профессиональных обязанностей
Задачи:	повышение уровня профессиональных компетенций за счет актуализации знаний и умений в области информационной безопасности; совершенствование и углубление профессиональных компетенций, необходимых для выполнения всех трудовых функций, возложенных на специалиста по информационной безопасности в соответствии с действующими нормативными правовыми актами;
Область профессиональной деятельности	Программа обучения разработана на основании профессионального стандарта «Специалист по защите информации в автоматизированных системах», утверждённого приказом Министерства труда и социальной защиты РФ № 367н от 27.04.2023 г.
Категория слушателей. (требования к квалификации слушателей):	Лица, имеющие высшее образование или среднее специальное образование в области информационных технологий, занятые в должностях специалистов по информационной безопасности предприятий, учреждений, организаций.
Срок освоения:	140 ч.
Режим занятий:	без отрыва/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***.**

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПК-1.1. Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

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

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 курса 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.

В результате обучения слушатель будет:

иметь представление:

- о современном состоянии, тенденциях и перспективах развития в области систем мониторинга и регистрации событий ИБ;
- о структуре и организации мониторинга и анализа событий и инцидентов информационной безопасности с использованием киберполигона Ampire;
- о системах обнаружения и предотвращения компьютерных атак;

быть способен:

- использовать программно-аппаратный комплекс ViPNet IDS;
- проводить мониторинг и анализ событий и инцидентов информационной безопасности, в том числе с использованием средств, входящих в состав киберполигона Ampire;
- проводить расследование инцидентов информационной безопасности, оценку защищённости элементов информационных систем и сетей;

знать и использовать:

- принципы работы систем обнаружения компьютерных атак;

- подсистемы обнаружения атак, подсистемы защиты от преднамеренных воздействий, контроля целостности информации;
- принципы действия, технологию использования и методику применения сетевого сенсора ViPNet IDS;
- методы мониторинга и анализа событий и инцидентов информационной безопасности с использованием средств киберполигона Ampire;

уметь:

- проводить аудит журналов на предмет попыток НСД и прочих нарушений;
- обоснованно выбирать необходимые программные и программно-аппаратные средства защиты информации;
- проводить мониторинг и анализ событий и инцидентов информационной безопасности с использованием средств киберполигона Ampire;
- организовывать поиск и использование оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении, а также других актуальных для обеспечения информационной безопасности данных;

владеть:

- технологией мониторинга и анализа событий и инцидентов информационной безопасности;
- методами и средствами выявления угроз безопасности информации, методиками выявления каналов утечки информации;
- оценкой эффективности предлагаемых и реализуемых организационно-технических решений по обеспечению безопасности информации;
- навыками по устранению уязвимостей в информационных системах общего и специального назначения

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: 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

2. УЧЕБНЫЙ ПЛАН И КАЛЕНДАРНЫЙ УЧЕБНЫЙ ПЛАН

2.1 Учебный план

№	Наименование предметов, курсов, дисциплин (модулей)	Всего часов	в том числе			Форма контроля
			ЛК	ПЗ	СР	
1	Модуль 1: Организационно-правовые основы обеспечения защиты информации в Российской Федерации	14	8	2	4	Контроль на ПЗ
2	Модуль 2. Современные средства анализа и поиска сетевых угроз и уязвимостей программно-аппаратного обеспечения автоматизированных систем	18	7	7	4	Контроль на ПЗ
3	Модуль 3: Решения по обнаружению, предотвращению компьютерных атак и интеллектуального	57	17	28	12	Контроль на ПЗ

	анализа событий и автоматического выявления инцидентов на базе продуктов Infotecs.					
4	Модуль 4: Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения «Ampire»	40	3	30	7	Контроль на ПЗ
	Итоговая аттестация	11	-	-	11	Тестирование
Итого		140	35	67	38	

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					6 часов в день					6 часов в день					
1	**Модуль 1.** Организационно-правовые основы обеспечения защиты информации в Российской Федерации	**Т**	**Т**	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х
2	**Модуль 2**. Современные средства анализа и поиска сетевых угроз и уязвимостей программно-аппаратного обеспечения автоматизированных систем	Х	Х	**Т**	**Т**	**Т**	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х
3	**Модуль 3.** Решения по обнаружению, предотвращению компьютерных атак и интеллектуального анализа событий и автоматического выявления инцидентов на базе продуктов Infotecs.	Х	Х	Х	Х	**Т**	**Т**	**Т**	**Т**	**Т**	**Т**	**Т**	Х	Х	Х	Х	Х
4	**Модуль 4.** Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения «Ampire»	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	**Т**	**Т**	**Т**	**Т**	**Т**
5	**Итоговая аттестация**	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	Х	**И**

[1]Даты обучения будут определены в расписании занятий при наборе группы на обучение
□– учебная неделя; Т – теоретическое обучение; А – промежуточная аттестация; И –итоговая аттестация; × – нет занятий

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

3.1 Рабочая программа дисциплины «ОБНАРУЖЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА БАЗЕ ПРОГРАММНОГО КОМПЛЕКСА «AMPIRE»

3.1.1 Пояснительная записка

Цель:	повышение теоретической и практической подготовки обучаемых в области защиты информации и защищенных компьютерных сетей, а также приобретение умений и навыков работы с системами обнаружения и анализа компьютерных атак, приобретение навыков работы с киберполигоном для исследований инцидентов информационной безопасности,

	отработка алгоритмов группового взаимодействия, реализации защитных мер по устранению найденных недостатков информационной безопасности.
В результате изучения слушатели должны:	
знать:	принципы функционирования киберполигона, принципы работы систем обнаружения компьютерных атак; т ехнологию 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.
уметь:	проводить аудит журналов на предмет попыток НСД и прочих нарушений; обоснованно выбирать необходимые программные и программно-аппаратные средства защиты информации; проводить мониторинг и анализ событий и инцидентов информационной безопасности; организовывать поиск и использование оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении, а также других актуальных для обеспечения информационной безопасности данных.
владеть:	технологией мониторинга и анализа событий и инцидентов информационной безопасности; методами и средствами выявления угроз безопасности информации; навыками по устранению уязвимостей в информационных системах общего и специального назначения.

3.1.2 Учебно-тематический план

№	Наименование предметов, курсов, дисциплин (модулей)	Всего часов	в том числе			Проверка знаний
			ЛК	ПЗ	СР	
1	Модуль 1: Организационно-правовые основы обеспечения защиты информации в Российской Федерации	14	8	2	4	Контроль на ПЗ
2	Модуль 2. Современные средства анализа и поиска сетевых угроз и уязвимостей программно-аппаратного обеспечения автоматизированных систем	18	7	7	4	Контроль на ПЗ
3	Модуль 3: Решения по обнаружению, предотвращению компьютерных атак и интеллектуального анализа событий и автоматического выявления инцидентов на базе продуктов Infotecs.	57	17	28	12	Контроль на ПЗ
4	Модуль 4: Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения «Ampire»	40	3	30	7	Контроль на ПЗ
	Итоговая аттестация	11	-	-	11	Тестирование
Итого		140	35	67	38	

3.1.3 Содержание программы

МОДУЛЬ 1. Организационно-правовые основы обеспечения защиты информации в Российской Федерации

Наименование темы	Содержание темы
1. Правовые основы обеспечения безопасности информационных технологий	Законы Российской Федерации и другие нормативные правовые акты, руководящие и нормативно-методические документы, регламентирующие отношения субъектов в информационной сфере и деятельность организаций по защите информации. Защита информации ограниченного доступа, права и обязанности субъектов информационных отношений. Лицензирование деятельности, сертификация средств защиты информации и аттестация объектов информатизации. Требования руководящих документов ФСТЭК России и ФСБ России. Ответственность за нарушения в сфере защиты информации. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Организация защиты информации в системах и средствах информатизации и связи.
2. Организационная структура системы обеспечения безопасности информационных технологий	Цели создания системы обеспечения безопасности информационных технологий. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы. Политика безопасности предприятия. Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации. Система организационно-распорядительных документов по обеспечению безопасности информационных технологий.
3. Угрозы безопасности информации, обрабатываемой на объектах КИИ	Объекты КИИ. Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении значимых объектов КИИ. Модель угроз безопасности информации значимого объекта КИИ. Типовые угрозы безопасности информации для информационных систем, информационно телекоммуникационных сетей, автоматизированных систем управления. Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Способы реализации угроз безопасности информации и их последствия. Типовые компьютерные инциденты для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.
4. Методы защиты конфиденциальной информации при ее обработке на объектах информатизации	Классификация методов и средств защиты информации. Особенности защиты на разных уровнях ИС. Антивирусная защита. Системы идентификации и аутентификации. Системы разграничения доступа. Стеганографические и криптографические методы. Технология электронной подписи. Методы обнаружения и блокирования угроз информационной безопасности. Методы защиты в операционных системах. сетевые технологии защиты.

МОДУЛЬ 2. Современные средства анализа и поиска сетевых угроз и уязвимостей программно-аппаратного обеспечения автоматизированных систем

Наименование темы	Содержание темы

1. Современные метрики уязвимостей, классификации действий злоумышленников в сети.	Международный подход к выявлению и анализу уязвимостей. Базы данных, содержание уязыимости, в том числе: Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE). Общая система оценки уязвимостей (стандарт Common Vulnerability Scoring System (CVSS)). Глобально доступная база знаний о тактиках и методах противника, основанная на реальных наблюдениях (MITRE ATT&CK ®). Общее перечисление и классификация шаблонов атак, или CAPEC.
2. Средства поиска угроз и анализа трафика.	Снифферы (визуальный и экспертный анализ). Системы обнаружения вторжений (хостового типа и сетевые). Системы типа SIEM - ПО для анализа информации, собранной из различных источников для раннего обнаружения инцидентов (Max Patrol, Wazuh). Межсетевые экраны.
3. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire»	Основное назначение ПК «Ampire», состав. Функциональные возможности. Типовой шаблон. Группа реагирования. Группа мониторинга (защиты). Цели, задачи. Критерии оценки. Мониторинг и анализ событий информационной безопасности. Шаблон, структура информационной системы предприятия. предприятия. Карточки инцидентов информационной безопасности, создание и особенности заполнения. Описание интерфейса ПК «Ampire». Распределение по группам. Панель тренировки. Статус уязвимостей. Сценарий тренировки - легенда киберучений.

МОДУЛЬ 3. Решения по обнаружению, предотвращению компьютерных атак и интеллектуального анализа событий и автоматического выявления инцидентов на базе продуктов Infotecs.

Наименование темы	Содержание темы
1. Технологии сбора информации. Технологии сканирования сети и детального сканирования сетевых узлов.	Способы применения сетевых сенсоров для анализа трафика: NMAP (ZENMAP), GREENBOON. Средства анализа сетевых пакетов WARESHARK. Применение средств имитации атакующих воздействий на основе решения METASPLOIT (ARMITAG).
2. Системы обнаружения вторжений уровня сети. Сетевой сенсор системы обнаружения атак ViPNet IDS NS	Виды систем обнаружений вторжений. Классификация по способам реагирования. Классификация по способам размещения. Классификация по методам анализа. Основные функции и принцип работы IDS NS. Состав, характеристики. Методы анализа данных. Мониторинг событий. Просмотр журнала событий. Настройка журнала.
3. Системы обнаружения вторжений уровня узла Система обнаружения вторжений ViPNet IDS HS	Назначение и состав системы обнаружения вторжений IDS HS. Функциональность. Принцип работы и порядок взаимодействия компонентов. Методы анализа данных в IDS HS.
4. Работа с системой централизованного	Управление структурой и настройками сенсоров; Управление конфигурациями правил; Мониторинг работоспособности сенсоров;

управления и мониторинга *ViPNet IDS MC*	Обновление: баз решающих правил; баз сигнатур вредоносного ПО; экспертных данных;
5. Основы администрирования системы интеллектуального анализа угроз безопасности информации программно-аппаратный комплекс ViPNet TIAS	Основные характеристики системы. Основные возможности. Принцип работы системы. Подходы к мониторингу и расследованию инцидентов. Предоставление руководству и контролирующим органам сводных отчетов по обнаруженным угрозам и инцидентам.

МОДУЛЬ 4. Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения «Ampire»

Наименование темы	Содержание темы
1. Киберучения на базе программного комплекса «Ampire»	Удаленное подключение к сетевому сенсору ПАК ViPNet IDS. Мониторинг, анализ и расследование инцидентов информационной безопасности. Просмотр и поиск записей журнала событий. Поиск инцидентов ИБ. Пошаговое отслеживание действий виртуального нарушителя в инфраструктуре предприятия. Экспорт файлов об инциденте. Создание карточки инцидента ИБ. Удаленное подключение к информационной структуре предприятия в соответствии с шаблоном. Работа в составе команды. Анализ и распределение карточек инцидентов ИБ. Пошаговый анализ действий виртуального нарушителя в инфраструктуре предприятия и их последствий, Выявление угроз безопасности информации и технических каналов утечки информации, обследование объекта ИС. Работа со специальным программным обеспечением для обнаружения и анализа событий ИБ. Устранение обнаруженных уязвимостей в ИС предприятия. Реализации защитных мер по устранению найденных недостатков ИБ.

3.1.4 Промежуточная аттестация по программе

Промежуточная аттестация по программе проводится в форме тестирования.

3.1.5 Обеспеченность образовательного процесса учебной литературой и информационными ресурсами

Материалы дисциплины для слушателей размещены – http://eios.klgtu.ru/mod ЭИОС КГТУ. Доступ к материалам осуществляется после регистрации на основании договора об оказании образовательных услуг по программе повышения квалификации.

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. Платформа VulDB - база данных уязвимостей https://vuldb.com/
10. Веб-интерфейс для данных об уязвимостях CVE https://www.cvedetails.com/
11. Поиск информации/ База знаний на www.opennet.ru https://www.opennet.ru/search.shtml
12. База знаний о тактике и методах нарушителей https://attack.mitre.org/
13. Материалы базовых сценариев (zip-архивы);
14. 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.

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, 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 с применением дистанционных образовательных технологий.

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.

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 высшего профессионального образования 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

Лекционные и практические занятия проводятся на базе аудиторного фонда университета.

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.

Преподавателю следует акцентировать внимание на перечисленных условиях, при проведении занятий в форме ВКС обязательно провести инструктаж слушателей по техническим аспектам подключения к платформе, разъяснить порядок работы с ЭИОС.

Основные рекомендации по реализации ДПП сводятся к следующему:

Дать представление:

- о современном состоянии, тенденциях и перспективах развития в области систем мониторинга и регистрации событий ИБ;
- о структуре и организации мониторинга и анализа событий и инцидентов информационной безопасности;
- о системах обнаружения и предотвращения компьютерных атак;

научить:

- использовать программно-аппаратный комплекс ViPNet IDS;
- проводить мониторинг и анализ событий и инцидентов информационной безопасности;
- проводить расследование инцидентов информационной безопасности, оценку защищённости элементов информационных сетей;

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

Программа дополнительной профессиональной программы (программа повышения квалификации) **«Обнаружение, анализ и устранение последствий компьютерных атак на базе программного комплекса «Ampire»** утверждена на заседании учебно-методической комиссии Института цифровых технологий.

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

и.о. директор Института
цифровых технологий — М.В. Гоконаев

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 4ae0684d0d529bb9d0248a5b51302ea1
Владелец: Гоконаев Мирослав Валерьевич
Действителен: с 02.08.2024 по 26.10.2025