МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Казанский национальный исследовательский технологический университет»
(ФГБОУ ВО «КНИТУ»)
ИНСТИТУТ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
(ИДПО КНИТУ)

УТВЕРЖДАЮ
Директор ИДПО ФГБОУ ВО «КНИТУ»
_____ Ю.Н.Зиятдинова
03 сентября 2024 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Кибербезопасность»
(36 акад. часов)

Лицензия ФГБОУ ВО «КНИТУ» серия 90Л01, № 0009203, рег. №2165 от 27.05.2016

Программа утверждена на заседании учебно-методической комиссии ИДПО ФГБОУ ВО «КНИТУ» (протокол от 03 09 2024 г. № 9)

Председатель учебно-методической комиссии _____ В.В. Кондратьев

Программа утверждена на заседании Ученого совета ИДПО ФГБОУ ВО «КНИТУ» (протокол от 03. 09 .2024 г. № 7)

Председатель Ученого совета ИДПО ФГБОУ ВО «КНИТУ» _____ Ю.Н.Зиятдинова

Казань, 2024 г.

Цели обучения	Формирование у обучающихся знаний, умений и навыков в области кибербезопасности, заложить терминологический фундамент и ознакомить с специальными методами и подходами обеспечения кибербезопасности., необходимых для профессиональной деятельности работника в области защиты информации.
Планируемые результаты обучения	*знать:* –тактики и техники действий злоумышленника; –системы обнаружения вторжений; –способы управления уязвимостями –основные нормативные правовые акты в области моделирования угроз безопасности. *уметь:* – искать уязвимости в компьютерных системах; – закрывать найденные уязвимости; – пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; – выявлять и анализировать инциденты информационной безопасности на основе; *владеть:* – технологиями обнаружения признаков сетевых атак с помощью IDS/IPS; – навыками реагирования и расследования инцидентов
Формируемые компетенции:	Знание правовых основ организации защиты государственной тайны и конфиденциальной информации, методики оценки и разработки моделей угроз информационной безопасности систему организации комплексной защиты информации ограниченного доступа в системе, включая защиту персональных данных, технических каналов утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации, методов и способов несанкционированного доступа (НСД) к информации, способы и средства защиты от НСД к информации на объектах информатизации. Умение применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах. Проведение мониторинга эффективности программно-аппаратных средств обеспечения ИБ в КС. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации; в эксплуатации технических средств обеспечения информационной безопасности; Умение проводить анализ и оценивать угрозы информационной безопасности объекта разрабатывать концепции, политики и иные организационно-распорядительные документы, необходимые для эффективного функционирования комплексных систем информационной безопасности объектов информатизации в организации навыками применения средств антивирусной защиты. Навыки организации и обеспечения режима защиты информации; эксплуатации комплексов удостоверяющих центров;
Соответствие квалификационным требованиям	Программа составлена с учетом Постановления Минтруда РФ от 21.08.1998 N 37 (редакция от 15.05.2013) (разделы «Общеотраслевые квалификационные характеристики должностей работников, занятых на предприятиях, в учреждениях и организациях» и «Квалификационные характеристики должностей работников, занятых в научно-исследовательских учреждениях, конструкторских, технологических, проектных и изыскательских

	организациях»), приказа Минтруда России от 14.09.2022 N 525н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 14.10.2022 N 70543) и приказу Минтруда России от 14.09.2022 N 536н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (Зарегистрировано в Минюсте России 18.10.2022 N 70596).
Категория слушателей	- сотрудники подразделений обеспечения информационной безопасности, технической защиты конфиденциальной информации (ТЗКИ), ответственные за состояние и обеспечение ИБ и организацию работ по созданию комплексных систем защиты конфиденциальной информации предприятий; - сотрудники подразделений обеспечения информационной безопасности, технической защиты конфиденциальной информации (ТЗКИ), ответственные за состояние и обеспечение ИБ и организацию работ по созданию комплексных систем защиты конфиденциальной информации предприятий; - администраторы средств защиты и специалисты подразделений ОИБ (ТЗКИ), ответственных за защиту конфиденциальной информации техническими средствами.
Срок обучения	36 академических часов
Форма обучения	заочная с использованием дистанционных образовательных технологий и электронного обучения.

Календарный учебный график

Образовательный процесс по программе может осуществляться в течение всего учебного года. Занятия проводятся по мере комплектования групп.

Таблица 1

Форма обучения / **График обучения**	**Ауд. часов в день**	**Дней в неделю**	**Общая продолжительность программы (дней, недель, месяцев)**
заочная с использованием дистанционных образовательных технологий и электронного обучения	6	6	1 неделя

Учебный план

Таблица 2

Форма учебного плана программы, реализуемой в полном объеме с использованием аудиторных занятий

№	Наименование дисциплины	ОТ час.	СРС с ДОТ, час	Форма контроля
1	2	3	4	5
1	Раздел 1. Принципы построения защищенной ЛВС 1.1 Типовые корпоративные компьютерные сети и угрозы в сетях. Методы и средства защиты корпоративных компьютерных сетей	2	2	онлайн тесты
2	1.2 Изучение конкретной структуры корпоративной сети организации в шаблоне лаборатории "Киберполигон"	2	2	онлайн тесты
3	1.3 Мониторинг безопасности сетей. Снифферы. Системы обнаружения атак (IDS). Системы предотвращения атак (IPS). Системы предотвращения утечки информации (DLP). Мониторинг атак смоделированных на лаборатории "Киберполигон".	2	2	онлайн тесты
4	1.4 Выявление и устранение уязвимостей в информационных	2	2	онлайн тесты

	системах и компьютерных сетях. Выявление и устранение уязвимостей на примере лаборатории "Киберполигон"			
5	1.5 Расследование инцидентов в компьютерных сетях. Изучение перехваченного трафика, файлов журналов и т.д. Расследование атак.	2	2	онлайн тесты
6	Раздел 2. Практическая отработка сценариев на киберполигоне КНИТУ 2.1 Теоретические основы и прохождение сценария "Защита базы данных предприятия"	2	2	онлайн тесты
	2.2 Теоретические основы и прохождение сценария "Защита контроллера домена предприятия"	2	2	онлайн тесты
	2.3 Теоретические основы и прохождение сценария "Защита данных файлового сервера"	2	2	онлайн тесты
Итоговая аттестация		2	2	*Итоговое тестирование*
	Итого	36 часов	36	

* *ОТ – общая трудоемкость, Лк – лекции, ПЗ – практические занятия, СЗ – семинарские занятия, ЛЗ – лабораторные занятия, ДОТ – дистанционные образовательные технологии, СРС – самостоятельная работа слушателя*

Содержание учебных дисциплин (модулей)

Таблица 3

Форма содержания учебных дисциплин

№ п/п	Наименование тем	Содержание обучения по темам, наименование и тематика лабораторных (практических и/или семинарских) занятий, самостоятельной работы слушателя и используемых образовательных технологий
1.1	Типовые корпоративные компьютерные сети и угрозы в сетях. Методы и средства защиты корпоративных компьютерных сетей	Компьютерная сеть;сетевая модель OSI ISO;методы и средствы защиты корпоративных сетей, угрозы безопасности информации на различных объектах информатизации.
1.2	Изучение конкретной структуры корпоративной сети организации в шаблоне лаборатории "Киберполигон"	Цифровой двойник; три сценария зрелости организации и влиянии зрелости на состояние информационной безопасности, процесс работы в киберполигоне; функции группы мониторинга и реагирования;удаленное подключении к лаборатории; подключение к узлам шаблона сети.
1.3	Мониторинг безопасности сетей. Снифферы. Системы обнаружения атак (IDS). Системы предотвращения атак (IPS). Системы предотвращения утечки информации (DLP). Мониторинг атак, смоделированных на лаборатории "Киберполигон".	Способы мониторинга сетевой безопасности;снифферы; межсетевые экраны, IDS/IPS; протоколирование и аудит ИБ.
1.4	Выявление и устранение уязвимостей в информационных системах и компьютерных сетях. Выявление и устранение уязвимостей на примере лаборатории "Киберполигон"	Методы выявления и устранении уязвимостей; классификация уязвимостей OWASP, VipNet IDS NS; технологии обнаружения признаков сетевых атак с помощью IDS/IPS
1.5	Расследование инцидентов в компьютерных сетях. Изучение перехваченного трафика, файлов журналов и т.д. Расследование атак.	Процесс управления уязвимостями; схема этапов управления уязвимостями согласно стандартам РФ; процессы реагирования и расследования инцидентов ИБ, Cyber Kill Chain; базы знаний MITTRE ATT@CK.
2.1	Теоретические основы и прохождение сценария "Защита базы данных предприятия"	Уязвимости Content Management System (CMS); проблемы брутфорсинга паролей SSH; достоинства и недостатки MySQL, детектирование и устранение уязвимости Drupalgeddon2; просмотр логов подключений по SSH; фильтр и изучение содержимое файла .bash_history.
2.2	Теоретические основы и прохождение сценария "Защита контроллера домена предприятия"	Межсайтовый скриптинг; SQL-инъекциях; вредоносные скрипты web-shell, поиск и устранениеуязвимость к SQL-инъекциям;работа с

		Windows Defender; детектирование брутфорсинга подключения по RDP.
2.3	Теоретические основы и прохождение сценария "Защита данных файлового сервера"	Логирование событий в веб-сервере; проблемы безопасности MS Exchange;маршрутизатор pfSense.методы социальной инженерии; MS17-010, работа протокола SMBv1.
Итоговое тестирование		
Самостоятельная работа слушателя		Освоение теоретического и практического материала.
Используемые образовательные технологии		Электронное обучение на платформе LMS Moodle использованием видео контента, презентационных, текстовых материалов, тренировочных и проверочных тестов

Требования к промежуточной и итоговой аттестации

Итоговая аттестация производится *в форме онлайн тестирования.*

Лицам, успешно освоившим программу повышения квалификации и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Организационно-педагогические условия реализации ДПП

Материально-техническое обеспечение

Обучение проводится *с использованием электронной обучающей среды Moodle на платформе https://lms.idpo.knitu.ru/course/view.php?id=46*

Учебно-методическое обеспечение программы

Основная литература

1. Вострецова Е.В., Основы информационной безопасности : учебное пособие для студентов вузов. Екатеринбург : Изд-во Урал. ун-та, 2019. 204 с
2. Баланов А. Н. Комплексная информационная безопасность. Полный справочник специалиста. Практическое пособие. М.: Инфра-Инженерия. 2024. 156 с.
3. Васильева Т. Ю., Куприянов А. И., Мельников В. П. Информационная безопасность. Учебник. М.: КноРус. 2023. 372 с.
4. Гродзенский Я. С. Информационная безопасность. Учебное пособие. М.: РГ-Пресс. 2024. 144 с
5. Родичев Ю. А. Информационная безопасность. Национальные стандарты Российской Федерации. СПб.: Питер. 2021. 896 с.
6. Хорев П. Б. Программно-аппаратная защита информации. Учебное пособие. М.: Инфра-М. 2022. 327 с.
7. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. - Саров : РФЯЦ-ВНИИЭФ, 2019. 267 с

Дополнительная литература

1. Богомолова О.И., Мифтахова Л.Х., Тарасова О.В., Богомолов В.А., Плохотников С.П., Касимова А.Р., Информационные технологии / Казань: КНИТУ. 2016, с.157
2. Вострецова Е.В., Основы информационной безопасности : учебное пособие для студентов вузов. Екатеринбург : Изд-во Урал. ун-та, 2019. 204 с
3. Баланов А. Н. Комплексная информационная безопасность. Полный справочник специалиста. Практическое пособие. М.: Инфра-Инженерия. 2024. 156 с.

Нормативные правовые акты, профессиональные стандарты и т. п.

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
3. Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"
4. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ
5. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»
6. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»
8. Приказ ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

9. Приказ ФСТЭК РФ от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
10. Приказ ФСБ РФ от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
11. Приказ ФСБ РФ и ФСТЭК РФ от 31.08.2010 № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».
12. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).
13. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г.
14. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
15. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
16. Методика оценки угроз безопасности информации ФСТЭК.
17. Методические рекомендации по прохождению сценария на базе кибреполигона Ampire.
18. Матрица Mitre Att&CK Режим доступа https://attack.mitre.org/

Кадровое обеспечение программы

Таблица 4. Кадровое обеспечение.

№ п/п	Наименование дисциплин (модулей), разделов (тем, элементов и т.д.)	Фамилия, имя, отчество, год рождения	Ученая степень, ученое звание	Педагогический стаж	Основное место работы, должность
1	Принципы построения защищенной ЛВС	Сафиуллина Лина Хатыповна, 1989	к.т.н., доцент	11 лет	ФГБОУ ВО «КНИТУ, доцент
2	Принципы построения защищенной ЛВС. Практическая отработка сценариев на киберполигоне КНИТУ	Касимова Алина Ринадовна, 1993	Отсутствует	9 лет	ФГБОУ ВО КНИТУ, ст. преподаватель
3	Практическая отработка сценариев на киберполигоне КНИТУ	Сайфутдинов Руслан Альбертович, 1992	Отсутствует	3 года	ФГБОУ ВО КНИТУ, ст. преподаватель

Образовательный процесс обеспечивается кадрами, имеющими базовое образование, соответствующее профилю дисциплины, и систематически занимающимися профессиональной деятельностью по профилю дисциплины.

Разработчики программы:

Сафиуллина Лина Хатыповна, ученая степень: доцент, ученое звание: кандидат технических наук, доцент каф. ИБ КНИТУ

Касимова Алина Ринадовна, старший преподаватель кафедры ИБ КНИТУ

Сайфутдинов Руслан Альбертович, старший преподаватель кафедры ИБ КНИТУ

Руководитель программы
И.о. зав. каф. ИБ *Сафиуллина Л.Х.*