Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное
образовательное учреждение высшего образования
«Казанский (Приволжский) федеральный университет»

Департамент развития дополнительного образования
Отдел разработки, утверждения и реализации образовательных программ КФУ

УТВЕРЖДАЮ

Проректор
по дополнительному образованию

_____ И.А. Хайруллин
(подпись)

«____»_____ 2025 г.

Дополнительная профессиональная программа
повышения квалификации
Кибербезопасность для продвинутых пользователей

Категории слушателей:

- специалисты с высшим или средним профессиональным образованием в сфере информационных технологий, математики, физики и естественных наук;

Протокол заседания совместной комиссии Отдела планирования, аналитики и методической поддержки КФУ и Отдела разработки, утверждения и реализации образовательных программ КФУ № ___/2025 от ____2025г.

Директор ДРДО _____ И.В. Хашев

Казань – 2025

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы

Программа направлена на совершенствование следующих профессиональных компетенций:

- способность администрировать средства защиты информации в компьютерных системах и сетях (ПК-1);
- способность оценивать уровень безопасности компьютерных систем и сетей (ПК-2).

1.2. Планируемые результаты обучения

В результате освоения программы слушатель:

Должен знать:

- сущность и актуальность проблемы информационной безопасности;
- изучить концептуальные подходы к обеспечению информационной безопасности; угрозы информации, средства и методы обеспечения информационной безопасности.

Должен уметь:

- ориентироваться в проблемах информационной безопасности, методах и средствах защиты информации;

Должен владеть:

- теоретическими знаниями о принципах построения безопасных информационных систем;
- должны демонстрировать способность и готовность применять полученные знания в своей профессиональной деятельности.

1.3. Требования к уровню подготовки поступающего на обучение

К освоению дополнительных профессиональных программ допускаются лица, имеющие среднее профессиональное и (или) высшее образование

1.4. Программа разработана на основе

Профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» (утвержденного приказом Минтруда России от 14.09.2022 N 533н «Специалист по безопасности компьютерных систем и сетей»).

1.5. Форма обучения: онлайн, с применением электронного обучения и дистанционных образовательных технологий.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

Наименование раздела	Трудоемкость, час	Аудиторные занятия			СРС, час	Формы контроля и аттестации, час.
		Всего, час	в том числе			
			лекции	прак. занятия, семинары		
Раздел 1. Сущность, задачи информационной безопасности	4	2	2	–	2	–
Раздел 2. Методы контроля доступа к информации	14	8	4	4	6	–
Раздел 3. Математические основы защиты информации. Основные криптографические шифры	12	6	6	–	6	–
Раздел 4. Проблемы обеспечения безопасности ОС.	16	8	4	4	8	–
Раздел 5. Компьютерные вирусы и проблемы антивирусной защиты	8	4	4	–	4	–
Раздел 6. Задачи управления системой сетевой безопасности.	16	8	4	4	8	–
Всего	**70**	**36**	**24**	**12**	**34**	–
Итоговая аттестация	2	–	–	–	–	2
Итого	**72**	**18**	10	8	**16**	**2**

2.2. Календарный учебный график

Период обучения (дни, недели)[1)]	Наименование раздела/темы
1-я неделя	Раздел 1. Сущность, задачи информационной безопасности Раздел 2. Методы контроля доступа к информации
2-я неделя	Раздел 3. Математические основы защиты информации. Основные криптографические шифры Раздел 4. Проблемы обеспечения безопасности ОС.
3-я неделя	Раздел 5. Компьютерные вирусы и проблемы антивирусной защиты Раздел 6. Задачи управления системой сетевой безопасности

4-я неделя	Итоговая аттестация

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

2.3. Рабочие программы разделов

Наименование темы	Содержание лекций (количество часов)	Наименование практических занятий или семинаров (количество часов)	Виды СРС (количество часов)	Результат (формируемая ПК)
1	2	3	4	5
Раздел 1. Сущность, задачи информационной безопасности				
1.1. Введение в информационную безопасность	- основные понятия информационной безопасности - современная постановка задачи защиты информации - угрозы безопасности информационным системам и их классификация		Освоение лекционного материала	ПК-2
1.2. Методы защиты информации	- методы защиты информации - физические методы и средства защиты информации - аппаратные методы и средства защиты информации - программные методы и средства защиты информации	– настройка конфиденциальности в ОС Windows 10: настройка местоположения устройства, настройка вывода данных на заблокированный экран, отключение уведомлений с рекомендациями, отключение рекламного идентификатора - ограничение доступа к камере и микрофону в Windows 10	Освоение лекционного материала	ПК-1

		- проверка разрешений приложений в Windows 10 - ограничение доступа приложений к данным учетной записи в Windows 10		
Раздел 2. Методы контроля доступа к информации				
2.1. Классификация средств идентификации и аутентификации	1. Классификация средств идентификации и аутентификации с точки зрения применяемых технологий 2. Биометрия. Статические методы 3. Биометрия. Динамические методы	Настройка аутентификации в Windows 10: создание и управление учетными записями	Освоение лекционного материала	ПК-1
2.2. Технологии и протоколы аутентификации	– Технологии аутентификации – Протоколы аутентификации	Настройка биометрии в Windows 10	Освоение лекционного материала	ПК-1
Раздел 3. Проектирование взаимодействия пользователя с системой и дополнительные методы исследований				
3.1. Математические основы защиты информации.	– Модулярная арифметика. Малая теорема Ферма. Функция Эйлера. - Простые числа. Генерация простых чисел. Решето Эратосфена. - Вероятностные методы поиска простых чисел.		Освоение лекционного материала	ПК-2
3.2. Шифр Цезаря, шифр Виженера, шифры простой и сложной замены	– Шифр Цезаря - шифр Виженера - шифры простой и сложной замены		Освоение лекционного материала	ПК-2
3.3. Алгоритм RSA	– Расширенный алгоритм Евклида - Алгоритм быстрого возведения в степень по модулю		Освоение лекционного материала	ПК-2

	- Алгоритм RSA			
Раздел 4. Проблемы обеспечения безопасности ОС.				
4.1 Угрозы безопасности ОС	- Угрозы безопасности ОС - Понятие защищенной ОС	Отключение службы геолокации в Windows 10. Отключение голосовой активации в Windows 10.	Освоение лекционного материала	ПК-1
4.2 Подходы к построению защищенных ОС. Административные меры защиты	- Подходы к построению защищенных ОС - Административные меры защиты		Освоение лекционного материала	ПК-1
Раздел 5. Компьютерные вирусы и проблемы антивирусной защиты				
5. Компьютерные вирусы и проблемы антивирусной защиты	- Классификация компьютерных вирусов - Жизненный цикл вирусов - Основные каналы распространения вирусов и других вредоносных программ - Антивирусные программы и комплексы		Освоение лекционного материала	ПК-2
6. Задачи управления системой сетевой безопасности.				
6.1 Управление средствами сетевой безопасности	- Архитектура управления средствами сетевой безопасности - Основные понятия - Концепция глобального управления безопасностью	Настройка брандмауэра в Windows 10: настройка и управление сетями	Освоение лекционного материала	ПК-1

6.2	Функционирование системы управления средствами безопасности	- Глобальная и локальная политики безопасности - Функционирование системы управления средствами безопасности - Аудит и мониторинг безопасности	Настройка брандмауэра в Windows 10: настройка прав пользователей, групповых политик	Освоение лекционного материала	ПК-1

2.4. Оценка качества освоения программы (формы аттестации, оценочные и методические материалы)

2.4.1. Форма итоговой аттестации

Итоговая аттестация (зачет) проводится в виде итогового тестирования

Результаты аттестации отражаются в ведомости итоговой аттестации, которая подписывается всеми членами аттестационной комиссии.

2.4.2. Оценочные материалы

Слушатель получает по 5 вопросов из каждого раздела Программы.

Оценка результатов:

Форма контроля	**Критерии оценивания**	
	зачтено	**не зачтено**
Итоговое тестирование	Более 56% правильных ответов на вопросы	Менее 56% правильных ответов на вопросы (0-55%)

3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

3.1. Материально-технические условия

На компьютерном оборудовании должны быть установлены стандартные пакеты программ для видео-, аудио- демонстраций и просмотра презентаций в формате MS PowerPoint и PDF. Все иные необходимые для реализации ДПП ПК программные пакеты для ЭВМ должны быть установлены заблаговременно до начала реализации программы повышения квалификации

3.2. Учебно-методическое и информационное обеспечение

При организации программы необходимо предусмотреть и обеспечить равную доступность информационных (учебно-методических материалов) по направлению ДПП ПК для всех слушателей программы повышения квалификации.

По окончании программы слушателям предоставляется архив учебных и учебно-методических материалов по программе (в том числе, наработанных в процессе реализации программы самими слушателями) в электронной форме.

Основные источники:

1. Нестеров, С. А. Основы информационной безопасности: учебник / С. А. Нестеров. - 3-е изд., стер. - Санкт-Петербург : Лань, 2024. - 324 с. - ISBN 978-5-507-49077-6. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/370967 (дата обращения: 20.01.2024). - Режим доступа: для авториз. пользователей.
2. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. - Москва : ИНФРА-М, 2021. - 118 с. - (Высшее

образование: Бакалавриат). - DOI 10.12737/13571. - ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178152 (дата обращения: 20.01.2024). - Режим доступа: по подписке.
3. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР : ИНФРА-М, 2023. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1912992 (дата обращения: 20.01.2024). - Режим доступа: по подписке.

Дополнительные источники:

1. Мартынов, Л. М. Алгебра и теория чисел для криптографии / Л. М. Мартынов. - 3-е изд., стер. - Санкт-Петербург : Лань, 2024. - 456 с. - ISBN 978-5-507-48774-5. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/362942 (дата обращения: 20.01.2024). - Режим доступа: для авториз. пользователей.
2. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. - Москва : ИНФРА-М, 2024. - 216 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/2131865 (дата обращения: 20.01.2024). - Режим доступа: по подписке.
3. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. - 3-е изд., испр. и доп. - Москва : ИНФРА-М, 2022. - 327 с. - (Высшее образование: Бакалавриат). - DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598 (дата обращения: 20.01.2024). - Режим доступа: по подписке.
4. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. - Москва : ФОРУМ : ИНФРА-М, 2022. - 368 с. - (Среднее профессиональное образование). - ISBN 978-5-91134-360-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1836631 (дата обращения: 20.01.2024). - Режим доступа: по подписке.

Интернет-ресурсы:

1. Портал образовательных ресурсов по IT-технологиям - http://www.intuit.ru
2. Научная электронная библиотека - https://elibrary.ru/
3. Справочная система MSDN - http://msdn.com/

3.3. Кадровые условия

Для преподавателей ДПП ПК, обеспечивающих образовательный процесс, устанавливаются следующие обязательные (минимальные требования): наличие высшего образования, опыт преподавания по направлению образовательной программы.

3.4. Условия для функционирования электронной информационно-образовательной среды

Электронные информационные ресурсы	Вид занятий	Наименование оборудования, программного обеспечения
Яндекс.360: Телемост	Лекция, практические занятия	Компьютер, подключенный к сети Интернет, браузер, гарнитура

	или семинары	

4. РУКОВОДИТЕЛЬ И АВТОР(Ы) ПРОГРАММЫ

Руководитель: Васильев Александр Валерьевич, заведующий кафедрой системного анализа и информационных технологий Института вычислительной математики и информационных технологий КФУ.

Авторы:

Долгов Дмитрий Александрович, старший преподаватель кафедры системного анализа и информационных технологий Института вычислительной математики и информационных технологий КФУ.