Министерство науки и высшего образования Российской Федерации

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

Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ

Проректор
по дополнительному образованию

_____ И.А. Хайруллин
(подпись)

«____»_____ 2025 г.

Дополнительная профессиональная программа
повышения квалификации
Основы кибербезопасности

Утверждена Учебно-методической комиссией Института ВМиИТ КФУ

(протокол № 11 от «11» июля 2025 г.)

Председатель комиссии: А.А. Егорчев _____
(подпись)

Руководитель подразделения,
реализующего ДПО _____ А.А. Егорчев
(подпись) (инициалы, фамилия)

«____»_____ 20__ г.

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:

– значение информационной безопасности в структуре национальной безопасности.
– основы государственной политики в области информационной безопасности, понятийный аппарат информационной безопасности.
– принципы политики управления доступом подсистемы информационной безопасности объекта защиты.
– основы построения средств защиты информации прикладного и системного программного обеспечения.

Должен уметь:

– применять на практике основные общеметодологические принципы обеспечения информационной безопасности.
– находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства.
– решать задачи для разработки и реализации политики управления доступом в компьютерных системах и подсистемах информационной безопасности объекта защиты.
– применять на практике методы и средства защиты информации.

Должен владеть:

– базовыми методами и средствами обеспечения информационной безопасности.
– навыками анализа данных для выбора способов решения задач в области информационной безопасности.
– навыками внедрения и развития политики управления доступом в компьютерных системах.
– навыками анализа, выбора и администрирования средств защиты информации.

1.3. Требования к уровню подготовки поступающего на обучение

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

Категории слушателей:

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

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	6	4	2	2	2	–
Раздел 3. Математические основы защиты информации. Основные криптографические шифры	4	2	2	–	2	–
Раздел 4. Проблемы обеспечения безопасности ОС.	8	4	2	2	4	–
Раздел 5. Компьютерные вирусы и проблемы антивирусной защиты	4	2	2	–	2	–
Раздел 6. Задачи управления системой сетевой безопасности.	8	4	2	2	4	–
Всего	**34**	**18**	**12**	**6**	**16**	–
Итоговая аттестация	2	–	–	–	–	2
Итого	**36**	**18**	**12**	**6**	**16**	**2**

2.2. Календарный учебный график

Период обучения (дни, недели)[1)]	Наименование раздела/темы
1-й день	Раздел 1. Сущность, задачи информационной безопасности
2-3-й день	Раздел 2. Методы контроля доступа к информации
4-й день	Раздел 3. Математические основы защиты информации. Основные криптографические шифры
5-6-й день	Раздел 4. Проблемы обеспечения безопасности ОС.
7-й день	Раздел 5. Компьютерные вирусы и проблемы антивирусной защиты
8-9-й день	Раздел 6. Задачи управления системой сетевой безопасности

10-15-й день	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 (1 час)		Освоение лекционного материала (1 час)	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 (1 час)		Освоение лекционного материала (1 час)	ПК-1
Раздел 2. Методы контроля доступа к информации				
2.1. Классификация средств идентификации и аутентификации	– Классификация средств идентификации и аутентификации с точки зрения применяемых технологий – Биометрия. Статические методы – Биометрия. Динамические методы (1 час)	– настройка конфиденциальности в ОС Windows 10: настройка местоположения устройства, настройка вывода данных на заблокированный	Освоение лекционного материала Систематизация полученных практических навыков (1 час)	ПК-1

		экран, отключение уведомлений с рекомендациями, отключение рекламного идентификатора - ограничение доступа к камере и микрофону в Windows 10 - проверка разрешений приложений в Windows 10 - ограничение доступа приложений к данным учетной записи в Windows 10 (1 час)		
2.2. Технологии и протоколы аутентификации	– Технологии аутентификации – Протоколы аутентификации (1 час)	Настройка аутентификации в Windows 10: создание и управление учетными записями Настройка биометрии в Windows 10 (1 час)	Освоение лекционного материала Систематизация полученных практических навыков (1 час)	ПК-1
Раздел 3. Математические основы защиты информации. Основные криптографические шифры				
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. - шифр Цезаря		Освоение лекционного материала (2 часа)	ПК-2

	- шифр Виженера - шифры простой и сложной замены - Расширенный алгоритм Евклида - Алгоритм быстрого возведения в степень по модулю - Алгоритм RSA (2 часа)			
Раздел 4. Проблемы обеспечения безопасности ОС.				
4.1 Угрозы безопасности ОС	- Угрозы безопасности ОС - Понятие защищенной ОС (1 час)	Отключение службы геолокации в Windows 10. Отключение голосовой активации в Windows 10 (2 часа)	Освоение лекционного материала Систематизация полученных практических навыков (2 часа)	ПК-1
4.2 Подходы к построению защищенных ОС. Административные меры защиты	- Подходы к построению защищенных ОС - Административные меры защиты (1 час)		Освоение лекционного материала (2 часа)	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 (2 часа)		Освоение лекционного материала (2 часа)	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 (1 час)	Настройка брандмауэра в Windows 10: настройка и управление сетями (1 час)	Освоение лекционного материала Систематизация полученных практических навыков (2 часа)	ПК-1
6.2	Функционирование системы управления средствами безопасности	- Глобальная и локальная политики безопасности - Функционирование системы управления средствами безопасности - Аудит и мониторинг безопасности (1 час)	Настройка брандмауэра в Windows 10: настройка прав пользователей, групповых политик (1 час)	Освоение лекционного материала Систематизация полученных практических навыков (2 часа)	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 онлайн-тестирования.

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

2.4.2. Оценочные материалы

Слушатель получает 15 вопросов по содержанию Программы.

Примерные вопросы для тестирования

1. Из перечисленного, параметрами классификации угроз безопасности информации являются:
a)источники угроз
b)предпосылки появления
c)природа происхождения
d)степень прогнозируемости

2. Из перечисленного, группами требований к документированию системы защиты информации являются:
a)обработка угроз
b)протоколирование
c)тестирование программ
d)аутентификация;

3. _____ является содержанием параметра угрозы безопасности информации "конфиденциальность".
a)несанкционированное получение
b)уничтожение
c)искажение
d)несанкционированная модификация

4._____ является первым этапом разработки системы защиты ИС.
a)оценка возможных потерь
b)стандартизация программного обеспечения
c)изучение информационных потоков
d)анализ потенциально возможных угроз информации

5. Из перечисленного, угрозы безопасности по природе происхождения классифицируются как:
a)преднамеренная
b)случайная
c)объективная
d)субъективная

6. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство
a)доступность
b)восстанавливаемость
c)целостность

d)детермированность

7. Восстановление данных является дополнительной функцией услуги защиты
a)целостность
b)аутентификация
c)причастность
d)контроль доступа

8. Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство
a)аутентификация
b)причастность
c)доступность
d)контроль доступа

9. Из перечисленных свойств, безопасная система обладает:
a)доступность
b)детерминированность
c)конфиденциальность
d)целостность

10. Организационные требования к системе защиты
a)административные и процедурные
b)охрана территории предприятия и наблюдение за ней
c)физические средства
d)противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям

11. Требования к техническому обеспечению системы защиты
a)организационно-правовые мероприятия
b)аппаратурные и физические
c)организационно-технические
d)неформальные

12. _____ является наукой, изучающей математические методы защиты информации путем ее преобразования.
a)криптоанализ
b)стеганография
c)криптология
d)криптография

13. _____ называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.
a)шифром
b)электронной подписью
c)ключом
d)идентификатором

14. Искусственные угрозы безопасности информации вызваны:
a)деятельностью человека

b)ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
c)воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
d)корыстными устремлениями злоумышленников

15.Естественные угрозы безопасности информации вызваны:
a)деятельностью человека
b)ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
c)воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
d)корыстными устремлениями злоумышленников

Оценка результатов:

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

3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

3.1. Материально-технические условия

Наименование специализированных учебных помещений	Вид занятий	Наименование оборудования, программного обеспечения
Учебная аудитория ИВМиИТ КФУ	Лекции; практические занятия или семинары, СРС	Мультимедийный проектор, проекционный экран, акустическая система, стандартные пакеты программ для видео-, аудио-демонстраций и просмотра презентаций в формате MS PowerPoint и PDF, компьютер с доступом в «Интернет».

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.Мельников, Д.А. Информационная безопасность открытых систем : учебник / Д.А. Мельников. - 3-е изд., стер. - Москва : ФЛИНТА, 2019. - 444 с. - ISBN 978-5-9765-1613-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1042499 (дата обращения: 16.01.2025). - Режим доступа: по подписке.

2. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 16.01.2025). - Режим доступа: по подписке.

3. Нестеров, С. А. Основы информационной безопасности: учебник для вузов / 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: 16.01.2025). - Режим доступа: для авториз. пользователей.

4. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР : ИНФРА-М, 2024. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2140566 (дата обращения: 16.01.2025). - Режим доступа: по подписке.

5. 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: 16.01.2025). - Режим доступа: по подписке.

Дополнительные источники:

1. Мартынов, Л. М. Алгебра и теория чисел для криптографии: учебное пособие для вузов / 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: 16.01.2025). - 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: 16.01.2025). - 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: 16.01.2025). - 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: 16.01.2025). - 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. Образовательная платформа Stepik - https://stepik.org/

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 или семинары	Компьютер, подключенный к сети Интернет, браузер, гарнитура

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

Андрианова Анастасия Александровна, доцент кафедры системного анализа и информационных технологий Института вычислительной математики и информационных технологий КФУ.