ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дополнительная общеобразовательная программа

Кибербезопасность. СПО (базовый уровень)

Кибербезопасность. СПО (базовый уровень)

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Программа сочетает глубокую техническую подготовку с развитием командных навыков и правовой грамотности.

Содержание программы разработано с учётом возрастных особенностей целевой аудитории (обучающиеся учреждений среднего профессионального образования) и обеспечивают последовательное усвоение материала от базового синтаксиса Python до разработки и защиты итогового проекта.

Краткая характеристика программы

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Направление обучения: Современные языки программирования (в том числе для обеспечения информационной безопасности)

Уровень	Сроки	Формат	Объём
Базовый	1 учебный год (01.10.2026 – 28.05.2027)	Онлайн и офлайн	145 ак. часов

Аттестация

- Промежуточная (по модулям): 11 вариантов — тесты и практико-ориентированные задачи в тренажере
- Итоговая: 7 вариантов комплексных заданий — тест и защита проекта с презентацией

Учебно-методический комплект

- Презентации (теория + практика)
- Описания практических заданий и кейс-задач
- Задания для самоконтроля и самостоятельной работы
- Методические материалы для преподавателей
- Оценочные материалы всех уровней контроля

Практическая составляющая

- Практические задания различного уровня сложности
- 3 кейс-задачи (включая задачу от аккредитованной ИТ-организации)
- Проектная работа
- Вариативные, парные и групповые задания
- Задания на проверку и исправление ИИ-кода

Дополнительная ценность: связь с компетенциями ФГОС СПО

Особенности программы

Программа имеет техническую направленность. Цель: формирование у обучающихся практических навыков программирования на Python в контексте задач информационной безопасности, включая шифрование и хеширование данных, анализ веб-уязвимостей, работу с логами, а также разработку и защиту проекта.

Обучающиеся научатся использовать цифровые технологии осознанно и ответственно, критически оценивая риски, соблюдая культуру цифровой гигиены и понимая правовую ответственность специалиста по информационной безопасности.

Обучение построено на реальных кейсах ИТ-компаний, интерактивных тренажёрах с автоматической проверкой и проектной работе.

Программа ориентирована на вклад в развитие дальнейшей образовательной траектории в сфере ИТ за счёт включения элементов содержания, соответствующих общим и профессиональным компетенциям ФГОС СПО.

СТРУКТУРА ПРОГРАММЫ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Модуль 1. Вход в ИБ: право, мышление, базовые инструменты

№ темы	Название темы	Трудоемкость (ак. час)
Тема 1.1	Знакомство с платформой и ролями в ИБ	2
Тема 1.2	Ответственное использование ИТ: персональные данные, безопасность, цифровой след и этика ИИ	3
Тема 1.3	Как мыслит атакующий: шаги атаки и цифровой след	10
	Текущий контроль по 1 модулю	**1**
Тема 1.4	Безопасная разработка	5
Тема 1.5	Случайность в ИБ. Кейс-задача	14
	Промежуточная аттестация по 1 модулю	**1**

СТРУКТУРА ПРОГРАММЫ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Модуль 2. Прикладная защита данных: фишинг, шифрование, хеширование

№ темы	Название темы	Трудоемкость (ак. час)
Тема 2.1	Фишинг изнутри: письмо, легенда, триггеры	5
Тема 2.2	Шифрование и кодирование: от криптографии к битовым операциям	10
Тема 2.3	Хеширование и проверка целостности данных	5
	Текущий контроль по 2 модулю	**1**
Тема 2.4	Стеганография и анализатор подозрительных сообщений. Кейс-задача	5
Тема 2.5	Аутентификация и авторизация в информационных системах	10
	Промежуточная аттестация по 2 модулю	**1**

СТРУКТУРА ПРОГРАММЫ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Модуль 3. Защитник на практике: сети, веб, логи, CTF

№ темы	Название темы	Трудоемкость (ак. час)
Тема 3.1	Сети и веб: IP, порты, протоколы, заголовки	10
Тема 3.2	CSV-логи и выявление подозрительной активности	5
Тема 3.3	OWASP на понятном языке: XSS, SQL-инъекции и небезопасный ввод	4
	Текущий контроль по 3 модулю	**1**
Тема 3.4	Методы оценки защищённости информационных систем: где заканчивается обучение и начинается ответственность	10
Тема 3.5	Социальная инженерия. Кейс-задача	5
	Промежуточная аттестация по 3 модулю	**1**

СТРУКТУРА ПРОГРАММЫ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Модуль 4. Итоговый проект: инструмент для кибербезопасности на Python

№ темы	Название темы	Трудоемкость (ак. час)
Тема 4.1	Искусственный интеллект в атаках и защите	5
Тема 4.2	Методы командной проверки защищенности программных модулей	10
Тема 4.3	Выбор финального проекта: 3 варианта на выбор	5
	Текущий контроль по 4 модулю	**1**
Тема 4.4	Разработка и отладка проекта	8
Тема 4.5	Оформление проекта	5
	Промежуточная аттестация по 4 модулю	**1**
	Итоговый контроль	**1**

Планируемые результаты обучения

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

По окончании обучения по программе обучающиеся будут:

иметь представление:

- о триаде информационной безопасности
- об этических и правовых нормах деятельности в сфере информационной безопасности
- о принципах работы веб-уязвимостей и методах их нейтрализации
- о современных киберугрозах, включая социальную инженерию (фишинг) и атаки с использованием ИИ

знать:

- базовый синтаксис языка Python и стандартные модули для задач ИБ
- фундаментальные различия между кодированием, хешированием и шифрованием
- основные веб-уязвимости и принципы безопасной работы с пользовательским вводом
- принципы анализа сетевых логов и проверки базовых HTTP-заголовков безопасности

Планируемые результаты обучения

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

По окончании обучения по программе обучающиеся будут:

уметь:

- писать скрипты для шифрования и хеширования данных с использованием стандартных библиотек Python
- разрабатывать простые анализаторы логов для выявления подозрительной активности
- распознавать базовые веб-угрозы и применять методы их нейтрализации
- использовать модуль secrets для генерации криптостойких случайных значений
- работать с файловой системой

владеть:

- инструментами стандартной библиотеки Python
- навыками безопасной работы с файловой системой и пользовательскими данными
- методами отладки и тестирования программного кода (граничные случаи, обработка ошибок)
- базовыми навыками командной работы

Планируемые результаты обучения

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

По окончании обучения по программе у обучающегося будут сформированы:

- культура цифровой гигиены и ответственного поведения в сети
- понимание правовой ответственности и этических границ деятельности специалиста по информационной безопасности
- критическое мышление при работе с ИИ-инструментами
- навыки командной работы и распределения ролей
- первичные навыки формирования профессионального портфолио
- мотивация к дальнейшему изучению ИТ и информационной безопасности, профессиональному развитию и успешному трудоустройству в отрасли, в том числе к участию в профильных олимпиадах, соревнованиях и чемпионатах

Планируемые результаты обучения по программе направлены на формирование у обучающихся компетенций, предусмотренных ФГОС СПО по специальности 09.02.07 «Информационные системы и программирование».

Методы, формы и технологии, применяемые при реализации программы

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Методы обучения

Модульный, проблемный и контекстный подходы.

Формы занятий

Лекции с демонстрацией мультимедийных материалов, практические работы, самостоятельная работа.

Технологии

Традиционные (объяснительно-иллюстративные) и интерактивные (групповые обсуждения, решение кейсов).