МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет транспорта»
РУТ (МИИТ)
Институт управления и цифровых технологий

УТВЕРЖДАЮ

Директор Института управления
и цифровых технологий
РУТ (МИИТ)

_____ Е.С. Максимова
«7» июля 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

(программа повышения квалификации)

«ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»

по специальности – 09.03.01 «Информатика и вычислительная техника»

Москва 2025 г.

РАБОЧИЕ ПРОГРАММЫ МОДУЛЕЙ

МОДУЛЬ 1. Кибербезопасность – основные понятия.

Тема 1.1. Терминология в области кибербезопасности. Методы и практики защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

Тема 1.2. Основные факторы кибербезопасности. Безопасность компьютерных сетей. Безопасность приложений. Операционная безопасность. Процесс повышения осведомленности. Непрерывность ведения бизнеса.

МОДУЛЬ 2. Аутентификация, идентификация, авторизация

Тема 2.1 Контроль доступа – основные определения. Последовательность мер по контролю доступа к информационной системе. Понятия идентификации, аутентификации, авторизации.

Тема 2.2 Электронные ключи. Технологии электронных ключей. Электронные ключи Touch Memory – устройство и применение.

Тема 2.3 Технология RFID. Радиочастотная идентификация. RFID-метка – устройство и применение. Технология NFC.

Тема 2.4 Магнитные карты, штрих- и QR-коды. Карты с магнитной полосой. Технологии HiCo и LoCo. Штрих-код. QR-код.

МОДУЛЬ 3. Биометрия

Тема 3.1 Статические методы. Методы контроля доступа по отпечатку пальца. Контроль доступа по форме ладони. Контроль доступа по расположению вен. Контроль доступа по сетчатке глаза. Контроль доступа по радужной оболочке глаза.

Тема 3.2 Динамические методы. Методы контроля доступа к информационной системе по рукописному почерку, по клавиатурному почерку, по голосу.

МОДУЛЬ 4. Технологии аутентификации.

Тема 4.1. Двухфакторная и многофакторная аутентификация. Назначение многофакторной аутентификации. Многослойная защита. Аутентификационные факторы.

Тема 4.2. Смарт-карты. Устройство и классификация. Контактные смарт-карты с интерфейсом ISO 7816. Контактные смарт-карты с USB интерфейсом. Бесконтактные (RFID) смарт-карты. Применение смарт-карт. Считыватели для контактных смарт-карт.

Тема 4.3. Технологии Рутокен и eToken. Электронный идентификатор Рутокен, электронные ключи eToken и их применение.

МОДУЛЬ 5. Парольная аутентификация.

Тема 5.1. Достоинства и недостатки традиционной парольной аутентификации. Достоинства парольной аутентификации. Недостатки парольной аутентификации. Одноразовые пароли.

Тема 5.2 Хранение и применение паролей. Проблемы хранения паролей. Примеры алгоритмов хеширования. Метод «запрос-ответ». Метод «только ответ». Метод «синхронизация по событию».

МОДУЛЬ 6. Хэширование и пароли.

Тема 6.1 Хранение паролей. Проблема безопасного хранения паролей. Применение хэширования для безопасного хранения паролей.

Тема 6.2 Хэш-функции. Математические основы хэширования. Существующие стандарты и протоколы хэширования.

МОДУЛЬ 7. Протоколы сетевой аутентификации. Модели разграничения доступа.

Тема 7.1 Локальная аутентификация в операционной системе. Последовательность действий при аутентификации в современных операционных системах. Подсистема локальной безопасности LSA. Диспетчер учетных записей безопасности (SAM).

Тема 7.2 Протокол NTLM v2. Схема работы протокола NTLMv2 с контроллером домена.

Тема 7.3 Протокол аутентификации Kerberos. Централизованное хранение аутентификационных данных. Понятие Ticket (билет, удостоверение). Примеры реализации протокола Kerberos

Тема 7.4 Протоколы аутентификации для удалённого доступа к информационным ресурсам. Протокол аутентификации Remote Authentication Dial-in User Service (RADIUS) – терминология, состав, порядок работы, особенности применения.

Тема 7.5 Модели разграничения доступа. Классификация моделей разграничения доступа. Дискреционная модель разграничения доступа. Мандатная модель. Ролевая модель. Модель на основе атрибутов. Гибридные модели.

МОДУЛЬ 8. Вредоносное программное обеспечение. Рассматриваются отдельные виды современного вредоносного программного обеспечения. Рекламные программы. Backdoor-программы. Файлы со скрытыми расширениями. Фишинг. Программы-шутки. Bot-сети. Эксплойт. Скрытый майнер. Фарминг.

МОДУЛЬ 9. Уязвимости информационной системы и борьба с ними.

Тема 9.1 Уязвимости и их классификация. Определения. Причины и последствия уязвимостей. Классификации и реестры уязвимостей.

Тема 9.2 Системы обнаружения и предотвращения вторжений. Назначение IDS-систем. Признаки угроз. Классификация систем обнаружения атак. Система предотвращения вторжений.

Тема 9.2 Системы обеспечения информационной безопасности предприятия. Назначение SIEM-систем. Принципы работы SIEM-систем. Ситуационные центры управления информационной безопасностью (Security Operation Center, SOC).

МОДУЛЬ 10. Итоговая аттестация.

Оценка уровня освоения программы слушателями.

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Реализация учебной программы проводится в полном соответствии с требованиями законодательства Российской Федерации в области образования, нормативными правовыми актами, регламентирующими данные направления деятельности.

Требования к квалификации педагогических кадров, представителей предприятий и организаций, обеспечивающих реализацию образовательного процесса

Реализация образовательного процесса обеспечивается высококвалифицированным профессорско-преподавательским составом, имеющим высшее образование и отвечающим квалификационным требованиям, указанным в Едином квалификационном справочнике, утвержденном приказом Министерства здравоохранения и социального развития Российской Федерации от 11.01.2011 № 1н, требованиям профессионального стандарта «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 08.09.2015