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.

ОБЩИЕ ПОЛОЖЕНИЯ

Программа повышения квалификации «Основы кибербезопасности» (далее - программа) разработана в соответствии с требованиями приказа Министерства образования и науки Российской федерации от 24.03.2025 № 266 с учетом потребности ОАО «РЖД» в обучении специалистов по обработке данных и обслуживанию средств вычислительной техники.

Содержание программы соответствует нормам Трудового кодекса Российской Федерации, нормативных актов Российской Федерации, локальных актов РУТ (МИИТ).

Программа разработана на основании установленных квалификационных требований по должностям «Руководители служб и подразделений в сфере информационно-коммуникационных технологий», «Специалисты-техники по компьютерным сетям и системам» и «Системные аналитики», установленных Профессиональным стандартом 06.015 «Специалист по информационным системам», утвержденным приказом Министерства труда и социальной защиты Российской Федерации от 13 июля 2023 г. № 586н «Об утверждении профессионального стандарта "Специалист по информационным системам", и требований образовательной программы высшего образования - программы бакалавриата по специальности 09.03.01 – Информатика и вычислительная техника, утвержденной решением ученого совета РУТ(МИИТ) протокол №8 от 17.02.2021 г., введенной в действие приказом Ректора №142/а от 10.03.2021г. и к результатам освоения образовательных программ.

Программа разработана кафедрой «Вычислительные системы, сети и информационная безопасность» ИУЦТ РУТ (МИИТ).

ЦЕЛЕВАЯ УСТАНОВКА

Цель обучения:

– совершенствование компетенций, необходимых для профессиональной деятельности в области организации безопасной обработки данных с применением средств вычислительной техники и обеспечения контроля доступа к информационной системе;

– повышение профессионального уровня в рамках имеющейся квалификации.

Категория слушателей: лица, имеющие высшее образование; лица, получающие высшее образование; лица, имеющие среднее профессиональное образование; лица, получающие среднее профессиональное образование.

Должностная категория слушателей: системные администраторы, техники, лица, выполняющие обработку данных с применением средств вычислительной техники.

Форма обучения: заочная с применением дистанционных образовательных технологий.

Трудоемкость программы: 72 академических часа,
заочное обучение посредством системы дистанционного обучения СДО ОАО «РЖД» – 72 часа.

Сроки освоения программы: 42 календарных дня (6 недель).

Режим занятий: 2 - 8 часов в день.
заочно посредством системы дистанционного обучения СДО ОАО «РЖД»,
без отрыва от производства, 72 ак. часа, 6 недель.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

В ходе обучения дать слушателям теоретические и практические знания в области организации эффективной и безопасной обработки данных с применением средств вычислительной техники, результатом получения которых будет:

совершенствование профессиональных компетенций:

Перечень профессиональных компетенций	Характеристика профессиональных компетенций		
	перечень знаний	перечень умений	практический опыт
Способность администрировать процесс управления безопасностью сетевых устройств, программного обеспечения, средств обеспечения безопасности удаленного доступа.	1. Виды защиты информации, основные понятия и определения; - стандарты и нормативные документы оценки информационной безопасности (ИБ) программного обеспечения и средств вычислительной техники. 2. Типы атак и методы противодействия атакам. 3. Службы и механизмы безопасности. 4. Концепцию построения систем защиты информации	1. Применять на практике методы противодействия атакам, методы и средства защиты информации от несанкционированного доступа (НСД). 2. Определять технические каналы утечки информации и способы их закрытия. 3. Использовать на практике службы и механизмы безопасности. 4. Структурировать угрозы ИБ, определять модель угроз и модель нарушителя. 5. Администрировать процесс управления безопасностью. 6. Разрабатывать архитектуру и определять состав системы обеспечения информационной безопасности.	1. Навыки оценки вероятности возникновения угроз ИБ и проведения анализа рисков реализации угроз. 2. Навыки формирования политики безопасности. 3. Навыками применения инженерно-технических, программно-аппаратных и криптографических средств защиты информации.
Способность планировать и проводить регламентные работы по восстановлению сетевой инфокоммуникационной системы	1. Методы и средства конфигурирования и контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексами. 2. Порядок обслуживания криптографических средств защиты информации. 3. Методы и принципы проведения аудита информационной безопасности.	1. Контролировать работу подсистем и изменять конфигурационные параметры при необходимости. 2. Применять методы и средства контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексами,	1. Навыки по настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. 2. Навыки прогнозирования поведения подсистемы информационной безопасности объекта при изменении внешних воздействий.

		обслуживать технические средств защиты информации. 3. Организовывать и проводить аудит работоспособности и эффективности применяемых средств защиты информации.	3. Навыки эксплуатации подсистем управления информационной безопасностью предприятия построенных с использованием современного оборудования. 4. Навыки оценивания оптимальности выбора программно-аппаратных средств защиты информации.

УЧЕБНЫЙ ПЛАН

№ п/п	Наименование модулей	Трудо-емкость, ак. час.	Из них занятия								Форма аттестации, трудоем-кость, ак. час.
			лекцион-ного типа		семинарс-кого типа		практичес-кого типа		консультаци онного типа		
			О	***З***	***О***	***З***	***О***	***З***	***О***	***З***	
1	Кибербезопасность – основные понятия	7		7							
2	Аутентификация, идентификация, авторизация	8		8							
3	Биометрия	8		8							
4	Технологии аутентификации	8		8							
5	Парольная аутентификация	8		8							
6	Хэширование и пароли	8		8							
7	Протоколы сетевой аутентификации. Модели разграничения доступа.	8		8							
8	Стеганография	7		7							
9	Уязвимости информационной системы и борьба с ними	8		8							
10	Итоговая аттестация	2									2
	Всего учебных часов	**72**		**70**							**2**

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

№ п/п	Наименование модуля	Количество учебных часов по учебным неделям (Н)						Итого
		Заочное (дистанционное) обучение						
		Н1	Н2	Н3	Н4	Н5	Н6	
1.	Кибербезопасность – основные понятия	7						7
2.	Аутентификация, идентификация, авторизация	5	3					8
3.	Биометрия		8					8
4.	Технологии аутентификации		1	7				8
5.	Парольная аутентификация			5	3			8
6.	Хэширование и пароли				8			8
7.	Протоколы сетевой аутентификации. Модели разграничения доступа.				1	7		8
8.	Вредоносное программное обеспечение					5	2	7
9.	Уязвимости информационной системы и борьба с ними						8	8
10.	Итоговая аттестация						2	2
	Всего учебных часов	**12**	**12**	**12**	**12**	**12**	**12**	**72**

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

№ 608н, научными работниками, руководителями и специалистами профильных организаций и предприятий, имеющими большой опыт практической работы (свыше 5-ти лет) в области профессиональной деятельности, соответствующей направленности программы.

Количественно-качественная характеристика педагогических кадров, обеспечивающих образовательный процесс, отражена в следующей таблице:

Заведующие кафедрами, профессоры (имеющие ученую степень и/или ученое звание)	Доценты, старшие преподаватели, (имеющие ученую степень и/или ученое звание)	Научные работники	Иные категории преподавательского состава
1	5	2	2

Требования к информационным и учебно-методическим условиям

Для прохождения дистанционного модуля программы слушателю необходимо иметь стандартный персональный компьютер (ноутбук), который отвечает следующим минимальным аппаратным требованиям:

– разрешение экрана монитора должно быть не ниже 1024x768 пикселей. Оптимальным для работы с курсом является разрешение 1280×1024 пикселей;

– компьютер (ноутбук) должен быть подключен к сети (Internet или сеть передачи данных СПД ОАО «РЖД») со скоростью не ниже чем 1Mb/c;

– процессор с тактовой частотой не менее 1GHz;

– объём оперативной памяти более 512 Мб.

На компьютере обучаемого должны быть установлены следующие программные продукты:

– операционные системы Windows 2000/XP/Vista/7, MacOS, Ubuntu (или большинство линукс-подобных операционных систем);

– браузеры для доступа к содержимому курса: IE v 8, 9, 10, актуальные версии Chrome, Firefox или Yandex, Opera, Safari;

– плагин браузера Adobe Flash Player (v 10 или выше) для просмотра флеш-роликов в курсе;

– Adobe Acrobat для просмотра дополнительных материалов курса (документов в формате PDF);

– Microsoft Office (Word и Excel) для просмотра дополнительных материалов курса.

Слушатели получают на первом занятии краткую инструкцию по прохождению программы обучения. Дополнительные справочные и учебно-

методические материалы доступны слушателям для скачивания из СДО в процессе обучения.

Общие требования к организации образовательного процесса

Программа повышения квалификации проводится в заочной форме с применением дистанционных образовательных технологий.

Материалы для изучения (далее – Контенты) размещаются в Системе дистанционного обучения ОАО «РЖД» (СДО). Доступ к материалам программы осуществляется с использованием информационных технологий, технических средств, информационно-телекоммуникационных сетей СПД ОАО «РЖД» или Internet, обеспечивающих возможность самостоятельного изучения обучающимися материалов программы с рабочих мест или личных персональных компьютеров, а также их взаимодействия с педагогическими работниками, имеющими соответствующий применяемым технологиям уровень подготовки.

При обучении используются следующие технические комплексы, программы и иные средства, способствующие лучшему теоретическому и практическому усвоению программного материала:

1. Система дистанционного обучения ОАО «РЖД»;
2. Персональный компьютер обучаемого.

Для входа в СДО ОАО «РЖД» в строке браузера необходимо набрать адрес системы СДО: new.sdo.rzd (для сети СПД) или new.sdo.rzd.ru (для сети Internet). Доступ к материалам программы и СДО обеспечивается круглосуточно.

С помощью браузера обучаемый получает возможность изучать основной материал программы, а также скачивать или просматривать методические пособия и дополнительный учебный материал.

Доступ к СДО через браузер возможен только для зарегистрированных в системе пользователей. Регистрация слушателей производится соответствии с «Регламентом взаимодействия подразделений ЦД и учебных заведений при тиражировании Типовой методики обучения работников хозяйства перевозок ОАО «РЖД» с применением дистанционных образовательных технологий» (утв. распоряжением ОАО «РЖД» от 30 декабря 2016 года № 2842р). При регистрации обучаемый получает персональное «имя пользователя» (логин) и «пароль», которые следует использовать для последующих обращений к системе.

Выдача логина-пароля оформляется «Ведомостью выдачи пароля и логина для доступа к дистанционным программам обучения», которую подписывает организатор обучения и заместитель начальника НОЦ прогрессивных

технологий перевозочного процесса, интеллектуальных систем организации движения и комплексной безопасности на транспорте ИУЦТ РУТ (МИИТ).

Обеспечение идентификации личности обучающегося и контроля соблюдения условий проведения обучения производится путем аутентификации – проверки подлинности слушателя путём сравнения введённого им логина-пароля с логином-паролем, сохранённым в базе данных пользователей.

Доступ слушателей к материалам программы производится после успешной аутентификации.

При регистрации перед началом обучения слушателю необходимо заполнить и подписать согласие на обработку персональных данных. Согласие требуется для организации учебного процесса по повышению квалификации, оформления и выдачи документов о дополнительном профессиональном образовании.

Учебно-методическая помощь обучающимся оказывается профессорско-преподавательским составом путем размещения в базе данных соответствующего Контента методических материалов, а также в форме индивидуальных консультаций на основе встроенных возможностей обмена сообщениями в СДО. В качестве методических материалов слушателям предоставляется «Инструкция по порядку прохождения программы повышения квалификации», «Справка по интерфейсу электронных курсов», а также дополнительные методические материалы в зависимости от содержания Контента.

Этапы совершенствования компетенций:

1. Развитие, пополнение базы знаний.

По программе определен комплект обязательных и дополнительных учебно-методических материалов и гарантировано их наличие для всех обучающихся. Обучаемый получает возможность изучать размещённые в СДО материалы как самой программы, так и дополнительные учебные материалы. Обязательный для изучения материал курса в СДО разбит на разделы и подразделы, которые в свою очередь разбиты на слайды. На слайдах представлен материал для изучения по конкретной теме. Дополнительный материал для изучения собран в базе данных соответствующего Контента, а также в «Медиатеке нормативно-технических документов и образовательных медиаматериалов, применяемых для повышения квалификации и технической учебы работников железнодорожного транспорта», которая представляет собой классифицированное по различным категориям хранилище видеоматериалов, изображений, схем, презентаций, методических пособий и документов. Дополнительный материал доступен слушателю при нажатии на кнопку "Дополнительно", расположенной в нижней части каждого слайда.

2. Развитие навыков практического использования знаний.

Умения и навыки практического использования знаний формируются посредством изучения порядка действий в практических ситуациях, возникающих у обучаемых в их работе.

Умения формируются в ходе семинарских занятий, которые проводятся с использованием методов интенсивного обучения и направлены на развитие знаний и умений по совершенствуемым компетенциям.

Дополнительный материал для формирования практических навыков собран в Медиатеке и представляет собой видеофильмы и анимационные ролики по действиям работников движения в различных аварийных и нестандартных ситуациях.

3. Проверка усвоения материала.

Для закрепления изучаемого материала проводится промежуточный контроль (самотестирование) и итоговая аттестация в виде компьютерного тестирования на базе специального программного комплекса СДО.

Промежуточное тестирование (самотестирование) обучаемый проходит после полного (100%) изучения контента учебного модуля. Промежуточное тестирование позволяет слушателю проверить свой уровень знаний по изученному материалу и подготовиться к итоговому тестированию по курсу. Оценка по промежуточному тестированию носит информативный характер и при оценке более 70% свидетельствует о том, что материал модуля усвоен.

Каждый модуль дистанционного курса содержит объем знаний, необходимых для развития частью той или иной профессиональной компетенции. Уровень развития профессиональных компетенций, приобретенный слушателем в процессе изучения модуля дистанционного обучения, можно оценить при промежуточном тестировании. Учитывая структуру модулей дистанционного обучения, возможно установление следующей шкалы, отражающей уровень развития профессиональной компетенции у слушателя после изучения модуля дистанционного курса:

– 70%–79% – базовый уровень развития профессиональной компетенции;

– 80% – 89% – средний уровень развития профессиональной компетенции;

– 90% и выше – высший уровень развития профессиональной компетенции.

Обучение завершается итоговой аттестацией. К итоговой аттестации допускаются слушатели, освоившие учебный план в полном объеме.

Итоговая аттестация проводится на последней (седьмой) неделе обучения. В период обучения (первые шесть недель) доступ к материалам итоговой аттестации заблокирован.

Итоговая аттестация слушателя программы осуществляется в заочной форме в виде компьютерного тестирования на базе специального программного

комплекса СДО и предназначена для определения уровня усвоения результатов практической и теоретической подготовки.

К итоговой аттестации допускаются слушатели, освоившие учебный план в полном объеме. Если слушатель не выполнил учебный план на 100% (изучение учебного контента менее 100%, прохождение промежуточного тестирования (самотестирования) менее 100%, уровень промежуточного тестирования менее 70% хотя бы по одному из разделов), тьютор не открывает для этого слушателя доступ к итоговой аттестации.

Идентификация личности при допуске к итоговой аттестации производится путем аутентификации.

В ходе итоговой аттестации слушателю необходимо пройти компьютерный тест, содержащий не менее 20 вопросов с многовариантными ответами (четырьмя и более). Список вопросов формируется случайным образом из пула вопросов по всему материалу курса.

Вопросы, содержащиеся в билетах, имеют равный уровень сложности. Предлагаемые вопросы в виде тестов имеют один однозначно определяемый правильный ответ. Время на ответы ограничено (30 минут), в случае окончания времени, отведенного на тестирование, тестирование заканчивается с текущим результатом. В случае неудовлетворительного ответа на итоговый тест слушатель допускается к повторной сдаче через 14 дней. В течение этого времени слушателю открыт доступ к материалам дистанционного модуля курса.

При итоговом тестировании все верные ответы берутся за 100%, тогда отметка выставляется в соответствии с следующими критериями:

- 70-100% - материал усвоен, зачтено;
- менее 70% - материал не усвоен, требуется дополнительное обучение.

ФОРМЫ АТТЕСТАЦИИ

Оценка уровня знаний слушателей производится по результатам итоговой аттестации в виде компьютерного тестирования в форме, определенной Дополнительной профессиональной программой.

Форма итоговой аттестации – зачет.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Перечень вопросов для подготовки к итоговой аттестации:

1. Что такое кибербезопасность?
2. Как называется программа, которая способна создавать свои копии и внедрять их в файлы и системные области компьютера?
3. Укажите последовательность действий при локальной аутентификации в операционных системах Windows.
4. Какое свойство является главной отличительной чертой компьютерного вируса?
5. Опишите назначение протокола NTLMv2.
6. Как называется группа компьютеров, зараженных вирусом, которая по команде из Интернета выполняет атаку указанного сайта?
7. Опишите назначение протокола RADIUS.
8. К чему приводит DoS-атака на сайт в Интернете?
9. Дайте определение рекламным программам.
10. По каким признакам можно предположить, что компьютер заражен вирусом?
11. Опишите назначение SIEM-систем.
12. Отметьте объекты, которые могут быть заражены компьютерными вирусами.
13. Опишите назначение IDS-систем.
14. Отметьте все ситуации, в которых компьютер может быть заражен вирусом.
15. Опишите назначение IPS-систем.
16. Как могут распространяться вирусы?
17. Какие вредоносные программы могут заражать документы Word и Excel?
18. Что такое эксплойт?
19. Какое действие нужно выполнить в самом начале, если на компьютере обнаружен вирус?
20. Отметьте вредоносные программы, которые распространяются в компьютерных сетях.
21. Как называется цепочка байтов, характерная для определённого вируса?
22. Перечислите методы аутентификации.
23. Отметьте все правильные утверждения про антивирус-сканер.
24. Отметьте все правильные утверждения про антивирус-монитор.
25. Перечислите динамические методы биометрической аутентификации.

26. В чем недостатки антивирусов-мониторов?

27. Перечислите статические методы биометрической аутентификации.

28. Какие технологии применяются для контроля доступа к информационной системе.

СПИСОК ЛИТЕРАТУРЫ

№№ п/п	Наименование
1	Конституция Российской Федерации
2	Федеральные законы
2.1	Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ
2.2	Федеральный закон Российской Федерации «О персональных данных» от 27.07.2006 № 152-ФЗ
2.3	Федеральный закон Российской Федерации «О коммерческой тайне» от 29.07.2004 № 98-ФЗ
2.4	Федеральный закон Российской Федерации «Об электронной подписи» от 06.04.2011 № 63-ФЗ
2.5	Федеральный закон Российской Федерации «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ
2.6	ГОСТ 34.12-2018 — межгосударственный стандарт «Информационная технология. Криптографическая защита информации. Блочные шифры». Принят межгосударственным советом по метрологии, стандартизации и сертификации (протокол от 29 ноября 2018 г. №54).
2.7	ГОСТ 34.13-2018 — межгосударственный стандарт, который называется «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров». Принят межгосударственным советом по метрологии, стандартизации и сертификации (протокол от 29 ноября 2018 г. №54).
3.	Учебная литература
3.1	Кодирование и защита информации в документообороте: метод. указ. к практ. и лаб. раб. для студ. спец. Прикладная информатика (в экономике) по дисц. Информационная безопасность / В.И. Морозова, К.Э. Врублевский; МИИТ. Каф. Экономическая информатика. - М.: МИИТ, 2010. - 56 с.
3.2	Шифрование с открытым ключом: метод. указ. к лаб. раб. по дисц. Информационная безопасность и защита информации для студ. спец. Автоматизированные системы обработки информации и управления, Информационные системы и технологии / Э.И. Костюковская, А.М. Удалов; МИИТ. Каф. Автоматизированные системы управления. - М.: МИИТ, 2008. - 28 с.
3.3	Криптографическая защита компьютерной информации: метод. указ. к лаб. раб. по дисц. Теоретические основы компьютерной безопасности для студ., обуч. по напр. Информационная безопасность / Я. М. Голдовский, Б. В. Желенков, И. Е. Сафонова; МИИТ. Каф. Вычислительные системы и сети. - М.: МГУПС(МИИТ), 2013. - 36 с.
3.4	Информационная безопасность персональных компьютеров: учеб. пособие для студ. спец. САПР и строительных спец. по курсу Методы и средства защиты компьютерной информации. Ч.2 / В.Ю. Смирнов, О.В. Смирнова; МИИТ. Каф. САПР транспортных конструкций и сооружений.М.: МИИТ, 2010. - 88 с.

№№ п/п	Наименование
3.5	Разработка мер защиты информационных ресурсов в корпоративной сети с выходом в интернет: учебнометод. пособие по курс. работе для специалистов напр. Компьютерная безопасность / В. М. Алексеев; МИИТ. Каф. Управление и защита информации. - М.: РУТ(МИИТ), 2017. - 9 с.
3.6	Голиков А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2015. — 284 с.
3.7	Сидоренко В.Г., Скоробогатова Н.Н. Аспекты информационной безопасности: Учебное пособие. – М.: РУТ (МИИТ). 2018. – 64 с.
3.8	Привалов А.А. Обеспечение информационной безопасности, проектирования, создания, модернизации объектов информации на базе компьютерных систем в защищенном исполнении: Учебно-методическое пособие к курсовой работе. - М.: РУТ (МИИТ), 2018. – 48 с.
3.9	Технологии защиты информации в компьютерных сетях: Курс лекций / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов — Москва: Интуит НОУ, 2016. — 368 с

Разработчики программы:

Заведующий кафедрой «Вычислительные системы, сети и информационная безопасность», доцент, к.т.н. Б.В. Желенков

Доцент кафедры «Вычислительные системы, сети и информационная безопасность», к.т.н. Я.М. Голдовский