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
«27» июня 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
(программа повышения квалификации)

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

по специальности – 09.03.01 «Информатика и вычислительная техника»

Москва 2025 г.

ОБЩИЕ ПОЛОЖЕНИЯ

Программа повышения квалификации «Основы информационной безопасности» (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. 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 обработки данных с применением средств вычислительной техники;

– 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 контроля использования сетевых устройств и программного обеспечения	1. Основные понятия ИБ, структура мер в области ИБ, кратко описываются меры законодательного, административного, процедурного и программно-технического уровней. 2. Политика безопасности, её типовая структура, меры по выработке и сопровождению. 3. Меры безопасности, имеющие дело с человеческим фактором, основные принципы, помогающие успеху таких мер.	1. Анализировать данные по организации контроля использования сетевых устройств и программного обеспечения. 2. Оформлять документацию в рамках действующей политики безопасности.	1. Анализ современных требований к контролю использования сетевых устройств и программного обеспечения. 2. Анализ и контроль выполнения требований «цифровой гигиены» при доступе к рабочему месту.
Способность планировать и проводить регламентные работы по восстановлению сетевой инфокоммуникационной системы	1. Меры законодательного, административного, процедурного и программно-технического уровней. Российское и зарубежное законодательство в области ИБ. 2. Меры по защите информационной системы от вредоносного программного обеспечения.	1. Анализировать угрозы вредоносного программного обеспечения. 2. Планировать резервное копирование данных. 3. Выбирать программные средства, обеспечивающие профилактику ущерба от действия вредоносного программного обеспечения.	1. Анализ антивирусного программного обеспечения. 2. Навыки работы в условиях современных угроз информационной безопасности.

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	Информационная безопасность – основные понятия	7		7							
2	Вредоносное программное обеспечение	8		8							
3	Защита от вредоносных программ	8		8							
4	Брандмауэры и другие методы защиты	8		8							
5	Шифрование	8		8							
6	Хэширование и пароли	8		8							
7	Современные алгоритмы шифрования	8		8							
8	Стеганография	7		7							
9	Безопасность в глобальной сети Интернет	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.	Информационная безопасность – основные понятия	7						7
2.	Вредоносное программное обеспечение	5	3					8
3.	Защита от вредоносных программ		8					8
4.	Брандмауэры и другие методы защиты		1	7				8
5.	Шифрование			5	3			8
6.	Хэширование и пароли				8			8
7.	Современные алгоритмы шифрования				1	7		8
8.	Стеганография					5	2	7
9.	Безопасность в глобальной сети Интернет						8	8
10.	Итоговая аттестация						2	2
	Всего учебных часов	**12**	**12**	**12**	**12**	**12**	**12**	**72**

РАБОЧИЕ ПРОГРАММЫ МОДУЛЕЙ

МОДУЛЬ 1. Информационная безопасность – основные понятия.

Тема 1.1. Терминология в области информационной безопасности. Защита информации. Свойства информации. Доступность информации. Целостность (отсутствие искажений) информации. Конфиденциальность информации. Понятие уязвимости.

Тема 1.2. Основные средства обеспечения информационной безопасности. Технические средства защиты информации: замки, системы сигнализации и видеонаблюдения. Устройства, блокирующие возможные каналы утечки информации. Программные средства контроля доступа. Организационные меры обеспечения информационной безопасности.

МОДУЛЬ 2. Вредоносные программы

Тема 2.1 Вредоносное программное обеспечение – основные понятия. Термины, определения. Мотивы создания вредоносного программного обеспечения.

Тема 2.2 Симптомы и уязвимости. Характерные признаки заражения. Файлы, наиболее уязвимые для заражения. Пути распространения вредоносного программного кода.

Тема 2.3 Типы вредоносных программ. Классификация компьютерных вирусов. Сетевые черви и особенности их распространения. Троянские программы – методы маскировки вредоносного программного обеспечения.

МОДУЛЬ 3. Защита от вредоносных программ

Тема 3.1 Антивирусы. Методы обнаружения вирусов. Классификация антивирусных программ. Антивирусы-мониторы.

Тема 3.2 Антивирусы-сканнеры. Особенности применения антивирусов-сканеров. Защита по требованию. Сигнатурный анализ. Эвристический анализ.

Тема 3.3 Антивирусы-мониторы. Особенности применения антивирусов-мониторов. Программы постоянной защиты. Проверка «на лету». Блокировка характерных действий.

МОДУЛЬ 4. Брандмауэры и другие методы защиты. Виды, принципы и назначение межсетевых экранов. Резервное копирование. Цифровая гигиена. Порядок действий при подозрении на заражение вредоносным программным обеспечением.

МОДУЛЬ 5. Шифрование.

Тема 5.1. Обеспечение конфиденциальности информации с помощью

шифрования. Понятие о криптографическом закрытии данных. Шифрование. Криптоанализ. Классификация криптографических алгоритмов

Тема 5.2 Стойкость криптографического закрытия. Понятие криптостойкости. Различия в криптостойкости на примере простых криптографических алгоритмов.

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. Современные алгоритмы шифрования.

Тема 7.1 Современные криптоалгоритмы. Особенности стандарта ГОСТ 28147-89. Асисимметричное шифрование по алгоритму RSA.

Тема 7.2 Электронная подпись. Принцип действия цифровой подписи. Приложения для использования электронной подписи.

МОДУЛЬ 8. Стеганография. Скрытая передача информации. Распространенные методы стеганографии. Сокрытие информации в текстовых, графических, звуковых и видеофайлах. Цифровые водяные знаки.

МОДУЛЬ 9. Безопасность в глобальной сети Интернет.

Тема 9.1 Угрозы безопасности в глобальной сети. Классификация угроз в глобальной сети. Фишинг и борьба с ним. Мошенничество с помощью троянских программ.

Тема 9.2 Правила личной безопасности в глобальной сети. Использование учетной записи. Хранение паролей. Оплата через глобальную сеть. Ответственность и осторожность.

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. Как называется программа, которая способна создавать свои копии и внедрять их в файлы и системные области компьютера?
2. Какое свойство является главной отличительной чертой компьютерного вируса?
3. Как называется группа компьютеров, зараженных вирусом, которая по команде из Интернета выполняет атаку указанного сайта?
4. К чему приводит DoS-атака на сайт в Интернете?
5. По каким признакам можно предположить, что компьютер заражен вирусом?
6. Отметьте объекты, которые могут быть заражены компьютерными вирусами.
7. Отметьте все ситуации, в которых компьютер может быть заражен вирусом.
8. Как могут распространяться вирусы?
9. Какие вредоносные программы могут заражать документы Word и Excel?
10. Какое действие нужно выполнить в самом начале, если на компьютере обнаружен вирус?
11. Отметьте вредоносные программы, которые распространяются в компьютерных сетях.
12. Как называется цепочка байтов, характерная для определённого вируса?
13. Отметьте все правильные утверждения про антивирус-сканер.
14. Отметьте все правильные утверждения про антивирус-монитор.
15. В чем недостатки антивирусов-мониторов?
16. Как называется выманивание паролей для доступа на сайты
17. Интернета с помощью специально сделанных веб-страниц,
18. которые внешне выглядят так же, как «официальные» сайты?
19. Как называется нежелательная реклама, которая рассылается по электронной почте?
20. Как называется программа, блокирующая передачу данных по каналам связи, которые часто используют вирусы и программы для взлома сетей?

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.
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.

№№ п/п	Наименование
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.

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