Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный университет технологий и управления им. К.Г. Разумовского (Первый казачий университет)»
(ФГБОУ ВО МГУТУ им. К.Г. Разумовского (ПКУ))

«УТВЕРЖДАЮ»
Директор
_____ О.В. Керимова
(подпись)
«___» _____ 2023 г.

Дополнительная профессиональная образовательная программа
профессиональной переподготовки

«Информационная безопасность»

(520 часов)

Пенза 2023 г.

Дополнительная профессиональная образовательная программа профессиональной переподготовки (далее – «Программа») (с применением дистанционных образовательных технологий) *«Информационная безопасность»* разработана рабочей группой в составе:
Акимова И.В. к.п.н., доцент;
Тусков А.А. к.т.н. доцент;
Грошева Е.С.

Дополнительная профессиональная образовательная программа профессиональной переподготовки составлена на основании профессионального стандарта/квалификационных требований *06.033 Специалист по защите информации в автоматизированных системах*
(наименование области профессиональной деятельности)

2523 Специалисты по компьютерным сетям

(укрупненные группы специальностей)

Согласовано:
Заместитель директора по УМР _____М.К. Сайфетдинова

Начальник УО _____Е.А. Гусарова

Руководитель цента ДО _____Е.А. Гуреева

ОГЛАВЛЕНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ *4*
2. СОДЕРЖАНИЕ ПРОГРАММЫ *8*
3. ОЦЕНОЧНЫЕ СРЕДСТВА *14*
4.ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ... *166*
5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ *18*
6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ *19*

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации Программы

Формирование у слушателей профессиональных компетенций, необходимых для профессиональной деятельности в области информационной безопасности.

Обучение слушателей основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которым подвергается информация; вредоносными программами; защитой от компьютерных вирусов и других вредоносных программ; методами и средствами защиты информации; политикой безопасности компании в области информационной безопасности; стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; защитой информации в сетях; требованиями к системам защиты информации.

Актуальность разработки образовательной программы по изучению основ информационной безопасности вытекает из следующего противоречия: с одной стороны все возрастающий спрос на образовательные услуги в области информационной безопасности, с другой стороны неготовность общего образования быстро и гибко реагировать на изменение спроса на образовательные услуги, вследствие ограничения рамками общеобразовательных стандартов.

а) *Область профессиональной деятельности слушателя*, прошедшего обучение по программе профессиональной переподготовки для выполнения нового вида профессиональной деятельности «06.033 Специалист по защите информации в автоматизированных системах» включает:

Повышение защищенности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости.

б) *Объектами профессиональной деятельности являются:* программа, информационная угроза, безопасность.

в) В соответствии с указанной миссией программа преследует следующие *цели*:

- развитие и закрепление компетенций, определяющих способность к самостоятельной жизни, к дальнейшему повышению своей образованности после завершения программы и самосовершенствованию в выбранной области;
- развитие у слушателей профессиональных компетенций с учетом профиля подготовки, определяющих их профессиональную пригодность и способность адаптироваться к профессиональной деятельности в современном обществе;
- контроль качества подготовки и степени сформированности компетенций на всех этапах реализации программы;
- обеспечение гарантированной способности выпускников осуществлять профессиональную деятельность в организациях и учреждениях любой формы собственности.

Слушатель, успешно завершивший обучение по данной программе, должен решать следующие профессиональные *задачи* в соответствии с видами профессиональной деятельности:

62.09 Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая

Выполнять работы по обеспечению безопасного хранение, передачи, получения информации и взаимодействия с ней; распознавание угрозы безопасности, выявлять мошеннические схемы и вредоносные программы; возможность безопасно работать с персональной и корпоративной информацией; безопасно работать при удаленном подключении;

62.01 Разработка компьютерного программного обеспечения:

Выполнять разработку, модернизацию, тестирование и поддержку программного обеспечения; в том числе разработка структуры и содержания и/или написание компьютерной программы, необходимой для создания и реализации поставленной задачи.

1.2. Характеристика дополнительных профессиональных компетенций

Характеристика компетенций, подлежащих совершенствованию, и (или) перечень новых компетенций, формирующихся в результате освоения Программы

Компетенции	
индекс	описание
ДПК-1	способность использовать основы безопасности компьютерных систем и сетей, законы и стандарты, обеспечивающие информационную безопасность.
ДПК-2	использовать средства обеспечения безопасности в компьютерных системах и сетях
ДПК-3	способность выбирать и оценивать средства и инструменты реализации приложений в области информационной безопасности
ДПК-4	способность проектировать и разрабатывать приложения в области информационной безопасности

Требования к уровню подготовки, необходимому для освоения Программы: слушатель должен иметь документ о высшем или среднем профессиональном образовании. Слушатель должен предварительно изучить дисциплину «Информатика» и быть квалифицированным пользователем персональных компьютеров.

1.3 Требования к результатам освоения Программы

В качестве планируемых результатов освоения Программы приводятся:

Результаты обучения	
индекс	содержание
РО-1	Проводить техническое проектирование
РО-2	Проводить рабочее проектирование
РО-3	Проводить моделирование процессов и систем
РО-4	Оценивать надежность и качество функционирования объекта проектирования

б) области знаний, умений и навыков, которые формируют указанные компетенции.

Компетенция		**Результаты обучения**			
индекс	содержание компетенции	индекс	знать	уметь	владеть
ДПК-1	способность использовать основы безопасности компьютерных	РО-1	Сущность и понятие информационной безопасности, характеристику ее	Классифицировать защищаемую информацию по видам тайны и степеням	Навыками формирования требований к техническом

	систем и сетей, законы и стандарты, обеспечивающие информационную безопасность.		составляющих; место информационной безопасности в системе национальной страны; виды, источники защищаемой информации;	секретности; классифицировать основные угрозы безопасности информации;	у проекту выбором решений для проекта методами оценки качества технического проекта
ДПК-2	использовать средства обеспечения безопасности в компьютерных системах и сетях	РО-2	факторы, воздействующие на информацию при ее обработке в автоматизированных системах; жизненные ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности;	Выполнять реализацию комплекса средств автоматизации	Навыками разработки рабочей документации проекта ПО
ДПК-3	способность выбирать и оценивать средства и инструменты реализации приложений в области информационной безопасности	РО-3	Методологию IDEF0, DFD,ER	Выполнять моделирования технологических процессов в нотациях Гейн-Сарсона, Баркера	Навыками работы в прикладных программах AiiFusion, MS Visio
ДПК-4	способность проектировать и разрабатывать приложения в области информационной безопасности	РО-4	Знание основ теории надежности и критериев качества программного обеспечения	Оценивать степень связности и сцепления программных модулей проекта	Навыками определения среднего времени наработки на отказ

1.4. Требования к уровню подготовки поступающего на обучение, необходимому для освоения Программы

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

1.5. Срок освоения Программы

Срок освоения программы: всего 260 часа, из них самостоятельная работа слушателя (СРС) 130 часов, в том числе консультации 130 часа. Количество недель: 11

Форма обучения: заочная форма, с применением ДОТ.

При любой форме обучения учебная нагрузка устанавливается не более 26 часов в неделю, включая все виды аудиторной и внеаудиторной учебной работы слушателя.

1.6 Календарный учебный график

№ п/п	Наименование дисциплин (модулей)	ТО, дней	П, дней	ПА, дней	ИА, дней	Всего, дней
1	2	3	4	5	6	7
1.	Теоретические аспекты информационной безопасности	15	15			30
2	Методология защиты информации	11,5	11,5			23
5	Разработка проекта	6,5	6,5			13
	Итоговая аттестация	1			3	1
	Всего					66

Условные обозначения	
ТО	Теоретическое обучение
П	Практика
ПА	Промежуточная аттестация
ИА	Итоговая аттестация

1.7 Форма обучения

Форма обучения заочная с использованием дистанционных образовательных технологий.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

Основным документом Программы является учебный план.

Таблица 1 – Форма учебного плана

Наименование дисциплин (модулей)	Общая трудоемкость, час	Самостоятельная работа слушателя, час.				Форма аттестации (текущий контроль, промежуточная аттестация)
		Всего, час.	в т.ч. консульт. час	Лабораторные занятия	Занятия семинарского типа (практические занятия/семинары)	
1	2	3	4	5	6	7
1. Теоретические аспекты информационной безопасности	104	104	52	52		Зачет
2. Методы противодействия	208	208	104	104		Зачет
3. Использование для защиты информации алгоритмов с закрытым ключом	104	104	52	52		Зачет
4. Использование алгоритмов для защиты информации с открытым ключом	104	104	52	52		Зачет
Итого	520	520	260	260		
Итоговая аттестация	0,5 (на одного слушателя)					экзамен

2.2 Учебно-тематический план

Наименование дисциплин (модулей)	Общая трудоемкость, час	Самостоятельная работа слушателя, час.				Форма аттестации (текущий контроль, промежуточная аттестация)
		Всего, час.	в т.ч. консульт. час	Лабораторные занятия	Занятия семинарского типа (практические занятия/семинары)	
1	2	3	4	5	6	7
1. Теоретические аспекты информационной безопасности	**104**	**104**	**52**	**52**		**Зачет**
1.1 Угроза информационной безопасности	52	52	26	26		
1.2 Организационно-правовые методы информационной безопасности	52	52	26	26		
2. Методы противодействия	**208**	**208**	**104**	**104**		**Зачет**
2.1 Противодействие методам социальной инженерии	68	68	34	34		
2.2 Обеспечение безопасности банковских карт	68	68	34	34		
2.3 Обеспечение безопасности в сети Интернет	72	72	36	36		
3. Использование для защиты информации алгоритмов с закрытым ключом	**104**	**104**	**52**	**52**		**Зачет**
3.1 Простейшие методы шифрования с закрытым ключом	52	52	26	26		
3.2 Принципы построения блочных шифров с закрытым ключом	52	52	26	26		
4. Использование алгоритмов для защиты информации с открытым ключом	**104**	**104**	**52**	**52**		**Зачет**
4.1 Введение в криптографию с открытым ключом	52	52	26	26		

4.2 Основные положения теории чисел, используемые в криптографии с открытым ключом	52	52	26	26		
Итого	520	520	260	260		
Итоговая аттестация (междисциплинарный экзамен)	0,5 (на одного слушателя)					Экзамен

2.3. Содержание Программы

Раздел 1. 1. Теоретические аспекты информационной безопасности

1) Планируемые результаты обучения

В результате обучения слушатель должен:

Результаты обучения	
индекс	содержание
РО-1	Проводить техническое проектирование
РО-2	Проводить рабочее проектирование

2) Формируемые компетенции:

Изучение модуля направлено на развитие и формирование следующих компетенций:

Компетенции	
индекс	описание
ДПК-1	способность использовать основы безопасности компьютерных систем и сетей, законы и стандарты, обеспечивающие информационную безопасность.
ДПК-2	использовать средства обеспечения безопасности в компьютерных системах и сетях

3) Тема 1.1 Угроза информационной безопасности

Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).

Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности.

Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.

Тема 1.2 Организационно-правовые методы информационной безопасности

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности..

Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности.

Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности.

Руководящие документы Гостехкомиссии России. Структура требований безопасности.

Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем.

Международные стандарты информационной безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»). Основные положения Единых критериев. Функциональные требования и требования доверия. ПонятияПрофиля защиты и Проекта защиты.

Раздел 2. Методы противодействия

1) Планируемые результаты обучения

В результате обучения слушатель должен:

Результаты обучения	
индекс	содержание
РО-1	Проводить техническое проектирование
РО-2	Проводить рабочее проектирование
РО-3	Проводить моделирование процессов и систем
РО-4	Оценивать надежность и качество функционирования объекта проектирования

2) Формируемые компетенции:

Изучение модуля направлено на развитие и формирование следующих компетенций:

Компетенции	
индекс	описание
ДПК-1	способность использовать основы безопасности компьютерных систем и сетей, законы и стандарты, обеспечивающие информационную безопасность.
ДПК-2	использовать средства обеспечения безопасности в компьютерных системах и сетях
ДПК-3	способность выбирать и оценивать средства и инструменты реализации приложений в области информационной безопасности
ДПК-4	способность проектировать и разрабатывать приложения в области информационной безопасности

3) Тема 2.1 Противодействие методам социальной инженерии

Как подбираются пароли. Доверчивость пользователя. Желание к выгоде у пользователя. Боязнь пользователей. Желание помочь у пользователя. Метод от противного. Смешанные методы социальной инженерии.

Тема 2.2 Обеспечение безопасности банковских карт

История банковских пластиковых карт. Общее строение пластиковых карт. Методы кражи информации с пластиковых карт. Поведение при краже.

Тема 2.3 Обеспечение безопасности в сети Интернет

История развития сети Интернет. Сбор данных. Использование баннеров. Фишинг. Рассылка через системы мгновенных сообщений. Подставная работа. Зомбирование компьютера. Сервисы коротких ссылок

Раздел 3. Использование для защиты информации алгоритмов с закрытым ключом

1) Планируемые результаты обучения

В результате обучения слушатель должен:

Результаты обучения	
индекс	содержание
РО-1	Проводить техническое проектирование
РО-2	Проводить рабочее проектирование
РО-3	Проводить моделирование процессов и систем
РО-4	Оценивать надежность и качество функционирования объекта проектирования

2) Формируемые компетенции:

Изучение модуля направлено на развитие и формирование следующих компетенций:

Компетенции	
индекс	описание
ДПК-1	способность использовать основы безопасности компьютерных систем и сетей, законы и стандарты, обеспечивающие информационную безопасность.
ДПК-2	использовать средства обеспечения безопасности в компьютерных системах и сетях
ДПК-3	способность выбирать и оценивать средства и инструменты реализации приложений в области информационной безопасности
ДПК-4	способность проектировать и разрабатывать приложения в области информационной безопасности

3)

Тема 3.1 Простейшие методы шифрования с закрытым ключом

Общая схема симметричного шифрования. Методы замены. Методы перестановки

Тема 3.2 Принципы построения блочных шифров с закрытым ключом

Понятие композиционного шифра. Операции, используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования. Требования к блочному алгоритму шифрования. Сеть Фейштеля.

Раздел 4. Использование алгоритмов для защиты информации с открытым ключом

1) Планируемые результаты обучения

В результате обучения слушатель должен:

Результаты обучения	
индекс	содержание
РО-1	Проводить техническое проектирование

РО-2	Проводить рабочее проектирование
РО-3	Проводить моделирование процессов и систем
РО-4	Оценивать надежность и качество функционирования объекта проектирования

2) Формируемые компетенции:

Изучение модуля направлено на развитие и формирование следующих компетенций:

Компетенции	
индекс	описание
ДПК-1	способность использовать основы безопасности компьютерных систем и сетей, законы и стандарты, обеспечивающие информационную безопасность.
ДПК-2	использовать средства обеспечения безопасности в компьютерных системах и сетях
ДПК-3	способность выбирать и оценивать средства и инструменты реализации приложений в области информационной безопасности
ДПК-4	способность проектировать и разрабатывать приложения в области информационной безопасности

3)

Тема 4.1. Введение в криптографию с открытым ключом

Предпосылки создания методов шифрования с открытым ключом и основные определения. Односторонние функции. Использование асимметричных алгоритмов для шифрования. Цифровая подпись на основе алгоритмов с открытым ключом. Формирование секретных ключей с использованием асимметричных алгоритмов. Требования к алгоритмам шифрования с открытым ключом.

Тема 4.2. Основные положения теории чисел, используемые в криптографии с открытым ключом

Простые и составные числа. Основная теорема арифметики. Взаимно простые числа и функция Эйлера. Арифметика остатков и теория сравнений. Малая теорема Ферма. Наибольший общий делитель. Обобщенный алгоритм Евклида. Инверсия по модулю m.

3. ОЦЕНОЧНЫЕ СРЕДСТВА

Оценка качества освоения обучающимися дополнительных профессиональных программ включает: текущий контроль успеваемости, промежуточную аттестацию и итоговую аттестацию обучающихся. Нормативно-методическое обеспечение текущего контроля успеваемости и промежуточной аттестации обучающихся по ДПП осуществляется в соответствии с Положением о текущем контроле в «МГУТУ». Текущий контроль успеваемости и промежуточная аттестация обучающихся осуществляются в соответствии с Основными положениями бально-рейтинговой системы, Положением о текущем контроле успеваемости и промежуточной аттестации слушателей в «МГУТУ».

Текущий и итоговый контроль в форме тестирования программой не предусмотрен.

Форма итогового и текущего контроля – зачет устный опрос.

Итоговый контроль формируется путем случайной выборки от 2 до 6 вопросов (по одному из каждого блока).

Вопросы для промежуточной аттестации

Блок 1

1. Понятие информационной безопасности (ИБ). Основные составляющие ИБ.
2. Определения угроз. Классификация угроз.
3. Вредоносное программное обеспечение.
4. Примеры угроз.
5. Российское законодательство в области ИБ.
6. Закон «Об информации, информатизации, защите информации».
7. Закон «О лицензировании».
8. Закон «О цифровой подписи».
9. Понятия стандартов и спецификаций («Оранжевая книга»). Механизмы безопасности.
10. Классы безопасности.
11. Сетевые сервисы и механизмы безопасности. Администрирование средств безопасности.
12. Функциональные требования.
13. Требования доверия безопасности.
14. Документы Гостехкомиссии.
15. Административный уровень ИБ. Основные понятия. Политика безопасности.
16. Административный уровень ИБ. Программа безопасности. Синхронизация программы с
17. жизненным циклом системы.
18. Идентификация и аутентификация. Основные понятия. Парольная аутентификация.
19. Одноразовые пароли.
20. Сервер Kerberos.
21. Идентификация и аутентификация с помощью биометрических данных.
22. Управление доступом. Основные понятия.

Блок 2

23. Средства и методы осуществления кражи информации.
24. Федеральные законы.
25. Признаки заражения компьютера вирусом.
26. История возникновения антивирусных программ.

27. Механизм работы современных антивирусов.
28. Надежность антивирусных программ.
29. Основные моменты использования антивирусных программ.
30. История файерволлов.
31. Механизм работы файерволла.
32. Основные моменты использования файерволла.
33. Самые нашумевшие зловредные программы.
34. Опасные уязвимости.
35. Опасность кражи персональных данных с мобильных телефонов.
36. Противодействие методам социальной инженерии.
37. Обеспечение безопасности банковских карт.
38. Обеспечение безопасности в сети Интернет.

Блок 3

39. Основные понятия криптографии
40. Простейшие методы шифрования с закрытым ключом
41. Принципы построения блочных шифров с закрытым ключом
42. Алгоритмы шифрования DES и AES
43. Алгоритм криптографического преобразования данных ГОСТ 28147-89
44. Криптографические хеш-функции
45. Поточные шифры и генераторы псевдослучайных чисел
46. Введение в криптографию с открытым ключом
47. Основные положения теории чисел, используемые в криптографии с открытым ключом
48. Криптографические алгоритмы с открытым ключом и их использование

Блок 4

49. Электронная цифровая подпись
50. Совершенно секретные системы
51. Шифрование, помехоустойчивое кодирование и сжатие информации
52. Помехоустойчивое кодирование
53. Принципы сжатия данных
54. Электронная подпись на основе алгоритма RSA
55. Цифровая подпись на основе алгоритма Эль-Гамаля
56. Управление открытыми ключами
57. Принципы использования генераторов псевдослучайных чисел при потоковом шифровании
58. Генераторы настоящих случайных чисел в криптографии

Итоговая аттестация – междисциплинарный экзамен устный опрос.

Цель итоговой аттестации заключается в установлении соответствия уровня профессиональной подготовленности выпускника к решению профессиональных задач, а также требованиям к результатам освоения программы на основе профстандарта.

При сдаче итоговой аттестации слушатель должен показать свою способность и умение, опираясь на полученные углубленные знания, умения и сформированные

профессиональные компетенции, самостоятельно решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения. Слушатель, подтвердивший в рамках итоговой аттестации высокий уровень сформированности профессиональных компетенций, необходимых для решения профессиональных задач, оканчивает обучение по указанной программе уровня образования с получением диплома о переподготовке дающий право на ведение новой профессиональной деятельности в сфере *обеспечения информационной безопасности*.

4.ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

4.1 Нормативно-правовое обеспечение Программы

-Федеральные законы
-Приказы Министерства науки и высшего образования РФ
-ФГОС ВО по направлению подготовки
- Единый квалификационный справочник должностей руководителей

4.2 Кадровое обеспечение Программы

К реализации Программы привлекаются научно-педагогические работники (НПР), имеющие высшее образование, соответствующее профилю Программы, отвечающие квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональным стандартам, а также практические работники, осуществляющие трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности Программы, в соответствии со статьей 331 Трудового кодекса Российской Федерации.

4.3 Учебно-методическое и информационное обеспечение Программы

Обеспечение образовательного процесса учебной и учебно-методической литературой

Наименование дисциплины	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы
Теоретические аспекты информационной безопасности	**1.** Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] — Электрон. дан. — СПб.: Лань, 2016. — 324 с. — Режим доступа: http://e.lanbook.com/book/75515 — Загл. с экрана. **2.** Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] — Электрон. дан. — СПб.: Лань, 2017. — 324 с. — Режим доступа: http://e.lanbook.com/book/90153 — Загл. с экрана. **3.** Белов, Е.Б. Основы информационной безопасности. [Электронный ресурс] / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. — Электрон. дан. — М.: Горячая линия-Телеком, 2006. — 544 с. — Режим доступа: http://e.lanbook.com/book/5121 — Загл. с экрана.

	4. Малюк, А.А. Введение в информационную безопасность. [Электронный ресурс] / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М.: Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/book/5171 — Загл. с экрана. 5. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. [Электронный ресурс] / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова. — Электрон. дан. — М.: Горячая линия-Телеком, 2012. — 550 с. — Режим доступа: http://e.lanbook.com/book/5114 — Загл. с экрана.
Методы противодействия	**1.** Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] — Электрон. дан. — СПб.: Лань, 2016. — 324 с. — Режим доступа: http://e.lanbook.com/book/75515 — Загл. с экрана. **2.** Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] — Электрон. дан. — СПб.: Лань, 2017. — 324 с. — Режим доступа: http://e.lanbook.com/book/90153 — Загл. с экрана. **3.** Белов, Е.Б. Основы информационной безопасности. [Электронный ресурс] / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. — Электрон. дан. — М.: Горячая линия-Телеком, 2006. — 544 с. — Режим доступа: http://e.lanbook.com/book/5121 — Загл. с экрана. 4. Малюк, А.А. Введение в информационную безопасность. [Электронный ресурс] / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М.: Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/book/5171 — Загл. с экрана. 5. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. [Электронный ресурс] / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова. — Электрон. дан. — М.: Горячая линия-Телеком, 2012. — 550 с. — Режим доступа: http://e.lanbook.com/book/5114 — Загл. с экрана.
Использование для защиты информации алгоритмов с закрытым ключом	**1.** Бабаш, А. В. Криптография / А. В. Бабаш, Г. П. Шанкин; под ред. В. П. Шерстюка, Э. А. Применко. – М.: СОЛОН-Пресс, 2007. – 512 с. – (Аспекты защиты). **2.** Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие / О. Р. Лапонина; под ред. В. А. Сухомлина. – 2-е изд., испр. – М.: Интернет - Ун-т Информационных Технологий; М.: БИНОМ. Лаборатория знаний, 2007. – 531 с.: ил. – (Основы информационных технологий) . **3.** Фороузан, Б. А. Криптография и безопасность сетей: учебное пособие / Б. А. Фороузан; пер. с англ. А. Н. Берлина. – М.: Интернет – Ун-т Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. – 784 ил. – (Основы информационных технологий). **4.** Зефиров, С. Л. Управление инцидентами кибербезопасности: учебное пособие / С. Л. Зефиров, А. Ю. Щербакова. – Пенза: Изд-во Пенз. гос. ун-та, 2012. – 104 с.

	5. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Текст]: учебное пособие / В. Ф. Шаньгин. - М.: ДМК Пресс, 2008. - 544 с. **6.** Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко; под ред. В. Б. Бетелина. - 4-е изд. - М.: Интернет - Ун-т Информационных Технологий: БИНОМ. Лаборатория знаний, 2012. - 205 с.
Использование алгоритмов для защиты информации с открытым ключом	**1.** Бабаш, А. В. Криптография / А. В. Бабаш, Г. П. Шанкин; под ред. В. П. Шерстюка, Э. А. Применко. – М.: СОЛОН-Пресс, 2007. – 512 с. – (Аспекты защиты). **2.** Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие / О. Р. Лапонина; под ред. В. А. Сухомлина. – 2-е изд., испр. – М.: Интернет - Ун-т Информационных Технологий; М.: БИНОМ. Лаборатория знаний, 2007. – 531 с.: ил. – (Основы информационных технологий) . **3.** Фороузан, Б. А. Криптография и безопасность сетей: учебное пособие / Б. А. Фороузан; пер. с англ. А. Н. Берлина. – М.: Интернет – Ун-т Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. – 784 ил. – (Основы информационных технологий). **4.** Зефиров, С. Л. Управление инцидентами кибербезопасности: учебное пособие / С. Л. Зефиров, А. Ю. Щербакова. – Пенза: Изд-во Пенз. гос. ун-та, 2012. – 104 с. **5.** Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Текст]: учебное пособие / В. Ф. Шаньгин. - М.: ДМК Пресс, 2008. - 544 с. **6.** Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко; под ред. В. Б. Бетелина. - 4-е изд. - М.: Интернет - Ун-т Информационных Технологий: БИНОМ. Лаборатория знаний, 2012. - 205 с. **1.**

5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Образовательное учреждение, реализующее данную программу располагает материально-технической базой, включая учебно-научные помещения и лаборатории в достаточной мере оснащены приборами и оборудованием естественнонаучного, общепрофессионального и специального назначения современную вычислительную технику, в том числе объединенную в локальную сеть, имеет выход в глобальные сети электронной коммуникации. Материальная база соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов учебных занятий.

Слушатели имеют возможность в процессе обучения пользоваться материальной базой ФГБОУ ВО МГУТУ им. К.Г. Разумовского (ПКУ):

- современным компьютерным классом с актуальными программными средствами и доступом в интернет;
- учебно-методическими пособиями и материалами по учебным дисциплинам, курсовым и выпускным работам.

6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			