МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
Северо-Кавказский филиал

СОГЛАСОВАНО

Генеральный директор ООО «Промышленные системы автоматического управления»

_____ В.Г. Потемкин

«19» февраля 2021 г.

УТВЕРЖДАЮ:
Директор СКФ БГТУ
им. В.Г. Шухова

_____ В.Л. Курбатов

«24» февраля 2021 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

МДК 02.02 Криптографические средства и методы защиты информации

основной профессиональной образовательной программы – программы подготовки специалистов среднего звена
Специальность
10.02.05 Обеспечение информационной безопасности автоматизированных систем
(базовой подготовки)
Квалификация выпускника
Техник по защите информации
Срок обучения
3 года 10 месяцев

Минеральные Воды, 2021 г.

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного Приказом Министерства образования и науки РФ № 1553 от 09.12.2016 г.,
- Плана учебного процесса БГТУ им. В.Г. Шухова по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного в 2021 г.

Организация разработчик: СКФ ФГБОУ ВО «БГТУ им. В.Г. Шухова», Северо-Кавказский филиал

Составитель: старший преподаватель  О.А. Митюгова

ученая степень и звание | подпись | инициалы, фамилия

Рабочая программа обсуждена и рекомендована на заседании кафедры Экономических и естественно-научных дисциплин

название кафедры

«_24_» _февраля_ 2021 г., протокол №_7__

Заведующий кафедрой: к.пед.н.  И.В. Черкасова

ученая степень и звание | подпись | инициалы, фамилия

Согласовано с работодателями:

ФИО	***Должность, место работы***
Потемкин Владимир Григорьевич	Директор ООО «Промышленные системы автоматического управления»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

1.1. Цель и планируемые результаты освоения МДК 02.02. Криптографические средства и методы защиты информации

В результате изучения МДК 02.02. Криптографические средства и методы защиты информации профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами обучающийся должен освоить основной вид деятельности *Защита информации в автоматизированных системах программными и программно-аппаратными средствами* и соответствующие ему профессиональные и общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	**Защита информации в автоматизированных системах программными и программно-аппаратными средствами**
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.

1.2. Общие компетенции:

Код	**Наименование видов деятельности и профессиональных компетенций**
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; – учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; – работы с подсистемами регистрации событий.
уметь	– применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись
знать	– основные понятия криптографии и типовых криптографических методов и средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации.

2.СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Обязательная учебная нагрузка	146
в том числе:	
теоретическое обучение	76
лабораторные занятия	52
консультации	2
самостоятельная работа	10
промежуточная аттестация в форме дифференцированного зачета (5 семестр)	
промежуточная аттестация в форме экзамена (6 семестр)	6

2.2. Тематический план и содержание междисциплинарного курса «Криптографические средства и методы защиты информации»

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)	Объем часов
1	2	3
МДК 02.02. Криптографические средства и методы защиты информации		**146**
Введение	**Содержание учебного материала**	2
	Предмет и задачи криптографии. История криптографии. Основные термины	
Раздел 1. Математические основы защиты информации		
Тема 1.1. Математические основы криптографии	**Содержание учебного материала**	26
	Элементы теории множеств. Группы, кольца, поля.	
	Делимость чисел. Признаки делимости. Простые и составные числа.	
	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	
	Классы. Полная и приведенная система вычетов.	
	Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	
	Китайская теорема об остатках.	
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	
	Арифметические операции над большими числами.	
	Эллиптические кривые и их приложения в криптографии.	
	Тематика лабораторных занятий	6
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	
	Проверка чисел на простоту	
	Решение задач с элементами теории чисел.	

Раздел 2. Классическая криптография		
Тема 2.1. Методы криптографического защиты информации	**Содержание учебного материала**	8
	Классификация основных методов криптографической защиты. Методы симметричного шифрования	
	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	
	Методы перестановки. Табличная перестановка, маршрутная перестановка	
	Гаммирование. Гаммирование с конечной и бесконечной гаммами	
	Тематика лабораторных занятий	6
	Применение классических шифров замены	
	Применение классических шифров перестановки	
	Применение метода гаммирования	
Тема 2.2. Криптоанализ	**Содержание учебного материала**	6
	Основные методы криптоанализа. Криптографические атаки.	
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	
	Перспективные направления криптоанализа, квантовый криптоанализ.	
	Тематика лабораторных занятий	8
	Криптоанализ шифра простой замены методом анализа частотности символов	
	Криптоанализ классических шифров методом полного перебора ключей	
	Криптоанализ шифра Вижинера	
Самостоятельная работа обучающихся Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к лабораторным занятиям с использованием методических рекомендаций преподавателя, оформление отчетов к их защите.		2
Промежуточная аттестация по МДК 02.02 в форме дифференцированного зачета		-
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**	4
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
	Тематика лабораторных занятий	2
	Применение методов генерации ПСЧ	
Раздел 3. Современная криптография		
Тема 3.1. Кодирование	**Содержание учебного материала**	4

информации. Компьютеризация шифрования.	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	
	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	
	Тематика лабораторных занятий	8
	Кодирование информации	
	Программная реализация классических шифров	
	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**	4
	Общие сведения. Структурная схема симметричных криптографических систем	
	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	
	Тематика лабораторных занятий	2
	Изучение программной реализации современных симметричных шифров	
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**	4
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	
	Элементы теории чисел в криптографии с открытым ключом.	
	Тематика лабораторных занятий	4
	Применение различных асимметричных алгоритмов.	
	Изучение программной реализации асимметричного алгоритма RSA	
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**	2
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
	Тематика лабораторных занятий	6
	Применение различных функций хеширования, анализ особенностей хешей	
	Применение криптографических атак на хеш-функции.	

	Изучение программно-аппаратных средств, реализующих основные функции ЭП	
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	2
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	
	Тематика лабораторных занятий	4
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	
	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала**	4
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала**	4
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	
	Тематика лабораторных занятий	2
	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**	4
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
	Тематика лабораторных занятий	4
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	
	Реализация простейших стеганографических алгоритмов	
Самостоятельная работа обучающихся Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам,		8

главам учебных пособий, составленным преподавателем) Подготовка к лабораторным занятиям с использованием методических рекомендаций преподавателя, оформление отчетов к их защите. Анализ современных симметричных криптоалгоритмов. Анализ современных асимметричных криптоалгоритмов. Программная реализация современных криптоалгоритмов. Законодательство в области криптографической защиты информации. Перспективные направления криптографии	
Консультации	2
Промежуточная аттестация по МДК 02.02 в форме экзамена	6
Всего:	**146**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы междисциплинарного курса МДК 02.02. Криптографические средства и методы защиты информации профессионального модуля ПМ.02 должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие учебных кабинетов:

№ 21. Кабинет информатики. Лаборатория программных и программно-аппаратных средств защиты информации.

Оснащена информационными стендами, 10 компьютерами на базе процессора DualCore Intel Core i3, оперативной памятью 4ГБ и жестким диском 500 ГБ, локальной сетью с пропускной способностью 100 Мбит/с, операционная система Windows 7 (32-bit) , учебной доской; рабочим местом преподавателя; справочными пособиями;

медиатекой (мультимедиа разработки и презентации к урокам); дидактическими материалами; персональным компьютером с лицензионным программным обеспечением;

мультимедиа проектором; интерактивной доской

рабочими местами на базе вычислительной техники по одному рабочему месту на обучающегося, подключенными к локальной вычислительной сети и сети «Интернет»;

программным обеспечением сетевого оборудования; обучающее программное обеспечение; СУБД; CASE-средствами для проектирования базы данных;

инструментальной средой программирования;

пакетом прикладных программ

Кабинет информатики. № 21. Лаборатория технических средств защиты информации.

Оснащена информационными стендами, по 10 компьютеров на базе процессора DualCore Intel Core i3, оперативной памятью 4ГБ и жестким диском 500 ГБ, локальной сетью с пропускной способностью 100 Мбит/с, операционная система Windows 7 (32-bit) учебной доской, учебно-методическими пособиями, наглядными пособиями, стульями на 1 ученика 1 стул, столами 1 шт. на 2 человек,

Оснащена аппаратными средствами аутентификации пользователя; средствами защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок; средствами измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.); стендами физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов

3.2. Информационное обеспечение обучения

3.2.1 Основная литература:

1. Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учебник для студ. Учреждений сред. Проф. Образования / М.Е. Ильин, Т.И. Калинкина, В.Н. Пржегорлянский. - Москва : "Академия", 2020. - 288 с.

2. Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2010. — 104 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17926.html. — Режим доступа: для авторизир. пользователей

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего

профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476997.

4. Бутакова, Н. Г. Криптографические методы и средства защиты информации : учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург : Интермедия, 2020. — 380 с. — ISBN 978-5-4383-0210-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161347. — Режим доступа: для авториз. пользователей.

3.2.2. Дополнительная литература:

1. Котов, Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов. — Новосибирск : Новосибирский государственный технический университет, 2016. — 59 с. — ISBN 978-5-7782-2959-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91377.html. — Режим доступа: для авторизир. Пользователей

2. Калмыков, И. А. Криптографические методы защиты информации : лабораторный практикум / И. А. Калмыков, Д. О. Науменко, Т. А. Гиш. — Ставрополь : Северо-Кавказский федеральный университет, 2015. — 109 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/63099.html. — Режим доступа: для авторизир. пользователей

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451933.

4. Хорев П. Б. Программно-аппаратная защита информации [Текст]: учеб. пособие / П. Б. Хорев. - 2-е изд., испр. и доп. – Москва : ФОРУМ, 2015. - 351 с.

3.2.3. Официальные, справочно-библиографические издания

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании

информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

11. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

12. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

14. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

15. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

16. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

17. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

18. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

19. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

20. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

21. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

22. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

27. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

29. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

39. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

40. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

41. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства

обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

42. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

45. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

48. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

49. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

50. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

3.2.4. Периодические издания:

1. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

2. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.2.5. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
МДК.02.02. Криптографические средства защиты информации

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных заданий, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторных занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно	- взаимодействие с обучающимися, преподавателями и	

взаимодействовать с коллегами, руководством, клиентами.	мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно	

	формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	