МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Димитровградский инженерно-технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
(ДИТИ НИЯУ МИФИ)

СОГЛАСОВАНО
От работодателя:
Зам. директора ООО "АИС Город"
должность, название предприятия
_____ А.Н. Насальник
«15» апреля 20 22 г.
М.П.

УТВЕРЖДАЮ
Руководитель ДИТИ НИЯУ МИФИ
должность и название образовательного учреждения
_____ И.И. Бегинина
«12» мая 20 22 г.
М.П.

РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА
МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
шифр, название модуля

ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ ВЗАЩИЩЕННОМ ИСПОЛНЕНИИ
шифр, название модуля

программы подготовки специалистов среднего звенапо специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем
код, наименование специальности

Форма обучения: очнаяУчебный цикл:профессиональный

Составители:А.С. Аверьянов, преподаватель техникума ДИТИ НИЯУ МИФИ
ФИО, преподаватель техникума ДИТИ НИЯУ МИФИ

Димитровград

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

1.1. Область применения программы

Программа учебной дисциплины является частью программы подготовки специалистов среднего звена (ППССЗ) в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасностиавтоматизированных систем.

Место дисциплины в структуре ППССЗ

Учебная дисциплина ММДК.02.02. Криптографические средства защиты информации по специальности 10.02.05 Обеспечение информационной безопасностиавтоматизированных систем относится к обязательной части ППССЗ и принадлежит к циклу профессиональных дисциплин и является базой для освоения профессиональных модулей (ПМ1- ПМ3).

1.2. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате освоения предмета студент должен:

Иметь практический опыт	- установки, настройки программных средств защиты информации в автоматизированной системе; - обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; - тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; - решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; - 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; - выявления событий и инцидентов безопасности в автоматизированной системе.

уметь	- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; - применять программные и программно-аппаратные средства для защиты информации в базах данных; - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; - применять математический аппарат для выполнения криптографических преобразований; - использовать типовые программные криптографические средства, в том числе электронную подпись; - применять средства гарантированного уничтожения информации; - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
знать	- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; - методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; - основные понятия криптографии и типовых криптографических методов и средств защиты информации; - особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

1.1.2. Перечень осваиваемых компетенций

Код	**Наименование видов деятельности и профессиональных компетенций**
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.

Профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.

Общие компетенции воспитания в рамках основных направлений воспитательной работы.

Код	**Наименование общих компетенций воспитания**
В17	Формирование чувства личной ответственности за научно-технологическое развитие России, за результаты исследований и их последствия
В19	Формирование научного мировоззрения, культуры поиска нестандартных научно-технических решений, критического отношения к исследованиям лженаучного толка
В25	Формирование творческого инженерного мышления, навыков организации коллективной проектной деятельности
В 26	Формирование культуры информационной безопасности
В 28	Формирование стремления к постоянному самосовершенствованию в сфере защиты информации в автоматизированных системах программными и программно-аппаратными средствами

1.3. Рекомендуемое количество часов на освоение программы дисциплины:
обязательной аудиторной учебной нагрузки обучающегося **198 часа**, из них :

- лекции 132 ч.;
- практические занятия 30 часов;
- курсовое проектирование 36 час;
- самостоятельная работа – 8 ч.;
- промежуточная аттестация – экзамен 10 час.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Количество часов***
Максимальная нагрузка	**162**
Обязательная аудиторная учебная нагрузка (всего)	**132**
в том числе:	
теоретические занятия	**42**
практические занятия	**60**
контрольные работы	**-**
Самостоятельная работа	**14**
Промежуточная аттестация в форме экзамена	**16**

1.1. Тематический план и содержание учебной дисциплины «МДК.02.01. Программные и программно-аппаратные средства 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	Коды компетенций, формированию которых способствует элемент программы
1	2	3	
Раздел 1. Математические основы защиты информации			
Тема 1.1. Введение. Математические основы криптографии	**Содержание**	**10**	ОК 01, 02, 09. ПК 2.2. ПК 2.4. В17-В 19, В25-В 26, В 28
	Предмет и задачи криптографии. История криптографии. Основные термины		
	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.		
	Практические занятия	**8**	
	Практическая работа № 1 Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	3	
	Практическая работа № 2.Проверка чисел на простоту	2	
	Практическая работа № 3. Решение задач с элементами теории чисел.	3	

Раздел 2. Классическая криптография			
Тема 2.1. Методы криптографического защиты информации	**Содержание**	**6**	ОК 01, 02, 09. ПК 2.2. ПК 2.4. ПК 2.1.ПК 2.2. ПК 2.3.ПК 2.4 .ПК 2.5.ПК 2.6. В17-В 19, В25-В 26 В 28
	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		
	Практические занятия	**8**	
	Практическая работа № 4. Применение классических шифров замены	3	
	Практическая работа № 5. Применение классических шифров перестановки	2	
	Практическая работа № 6. Применение метода гаммирования	3	
Тема 2.2. Криптоанализ	**Содержание**	**8**	ОК 01, 02,, 09. ПК 2.2. ПК 2.4. ПК 2.1.ПК 2.2. ПК 2.3.ПК 2.4 ПК 2.5.ПК 2.6. В17-В 19, В25-В 26 В 28
	Основные методы криптоанализа. Криптографические атаки.		
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса		
	Перспективные направления криптоанализа, квантовый криптоанализ.		
	Практические занятия	**6**	
	Практическая работа № 7. Криптоанализ шифра простой замены методом анализа частотности символов	2	
	Практическая работа № 8. Криптоанализ классических шифров методом полного перебора ключей	2	
	Практическая работа № 9. Криптоанализ шифра Вижинера	2	
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**	**6**	ОК 01, 02, 09. ПК 2.2. ПК 2.4. В17-В 19, В25-В 26 В 28
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии		
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.		
	Практические занятия	**3**	
	Практическая работа № 10. Применение методов генерации ПСЧ	3	
Раздел 3. Современная криптография			
Тема 3.1. Кодирование информации.	**Содержание учебного материала**	**6**	ОК 01, 02, 09. ПК 2.2. ПК 2.4.
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII		

Компьютеризация шифрования.	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств		В17-В 19, В25-В 26 В 28
	Практические занятия	**8**	
	Практическая работа № 11. Кодирование информации	3	
	Практическая работа № 12. Программная реализация классических шифров	2	
	Практическая работа № 13. Изучение реализации классических шифров замены и перестановки в программе CrypToolили аналоге.	3	
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**	**6**	ОК 01, 02, 09. ПК 2.2. ПК 2.4. В17-В 19, В25-В 26 В 28
	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		
	Практические занятия	**3**	
	Практическая работа № 14. Изучение программной реализации современных симметричных шифров	3	
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**	**8**	ОК 01, 02, 09. ПК 2.2. ПК 2.4. В17-В 19, В25-В 26 В 28
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.		
	Элементы теории чисел в криптографии с открытым ключом.		
	Практические занятия	**5**	
	Практическая работа № 15. Применение различных асимметричных алгоритмов.	2	
	Практическая работа № 16. Изучение программной реализации асимметричного алгоритма RSA	3	
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**	**6**	ОК 01, 02, 09. ПК 2.2. ПК 2.4. В17-В 19, В25-В 26 В 28
	Аутентификация данных. Общие понятия. ЭП. МАС. Однонаправленные хеш-функции. Алгоритмы цифровой подписи		
	Практические занятия	**8**	
	Практическая работа № 17. Применение различных функций хеширования, анализ особенностей хешей	3	
	Практическая работа № 18. Применение криптографических атак на хеш-функции.	2	
	Практическая работа № 19. Изучение программно-аппаратных средств, реализующих основные функции ЭП	3	
Тема 3.5.	**Содержание учебного материала**	**4**	ОК 01, 02, , 09.

Алгоритмы обмена ключей и протоколы аутентификации	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация		ПК 2.2. ПК 2.4. В17-В 19, В25-В 26 В 28
	Практические занятия	**5**	
	Практическая работа № 20. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2	
	Практическая работа № 21. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	3	
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала**	**6**	ОК 01, 02,09. ПК 2.2. ПК 2.4.
	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**	**2**	ОК 01, 02, 09. ПК 2.2. ПК 2.4. В17-В 19, В25-В 26 В 28
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер		
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.		
	Практические занятия	**3**	
	Практическая работа № 22. Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	3	
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**	**2**	ОК 01, 02, 09. ПК 2.2. ПК 2.4. В17-В 19, В25-В 26 В 28
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.		
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ		
	Практические занятия	**4**	
	Практическая работа № 23. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ Практическая работа № 24. Реализация простейших стеганографических алгоритмов	2 2	

Примерная тематика самостоятельной работы при изучении МДК.02.02 1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Программная реализация классических шифров 5. Методы механизации шифрования 6. Цифровое представление различных форм информации 7. Анализ современных симметричных криптоалгоритмов 8. Анализ современных асимметричных криптоалгоритмов 9. Программная реализация современных криптоалгоритмов 10. Сравнительный анализ функций хеширования 11. Аутентификация сообщений 12. Законодательство в области криптографической защиты информации 13. Перспективные направления криптографии 14. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) 15. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите. **консультации**	**7+7**	
Учебная практика МДК.02.01 **Виды работ:** - Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах - Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности - Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности - Составление документации по учету, обработке, хранению и передаче конфиденциальной информации - Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации - Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. - Устранение замечаний по результатам проверки Анализ и составление нормативных методических документов по обеспечению информационной безопасностипрограммно-аппаратными средствами, с учетом нормативных правовых актов. - Применение математических методов для оценки качества и выбора наилучшего программного средства **Учебная практика МДК.02.02** **Виды работ:** - Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи **консультации**	**144+16**	ОК 01, 02, 09. ПК 2.1- ПК 2.6. В17-В 21, В25-В 26, В 28

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие учебных кабинетов - лекционные аудитории с мультимедийным оборудованием; лаборатории «Программных и программно-аппаратных средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета - лекционная аудитория: посадочных мест - 30, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

Оборудование лаборатории «Программных и программно-аппаратных средств защиты информации» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- рабочее место преподавателя;
- учебно-методическое обеспечение модуля;
- интерактивная доска, комплект презентаций;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
- программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства криптографической защиты информации.

3.2. Информационное обеспечение обучения

Электронный ресурс

1. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563

2. Овчинников, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Овчинников. — Санкт-Петербург : ГУАП, 2021. — 133 с. — ISBN 978-5-8088-1591-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216491

3. Введение в криптографическую защиту информации объектов : учебник / С. Н. Ильиных, С. Г. Алюшина, Т. И. Калинкина [и др.]. — Москва : МТУСИ, 2021. — 276 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/215231

4. Сычев Ю.Н. Защита информации и информационная безопасность / Ю.Н. Сычев. - Москва : Инфра-М, 2021. - 201 с. - ISBN 978-5-16-016583-7. - URL: https://ibooks.ru/bookshelf/378002/reading

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ КОМПЕТЕНЦИИ

Контроль и оценка результатов освоения компетенции осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
1	***2***
В результате освоения учебной дисциплины обучающийся должен **уметь:** - получать информацию о параметрах компьютерной системы - подключать дополнительное оборудование и настраивать связь между элементами компьютерной системы - производить инсталляцию и настройку программного обеспечения компьютерных систем **Знать:** - базовые понятия и основные принципы построения архитектур вычислительных систем; - типы вычислительных систем и их архитектурные особенности; - организацию и принцип работы основных логических блоков компьютерных систем; - процессы обработки информации на всех уровнях компьютерных архитектур; - основные компоненты программного обеспечения компьютерных систем; - основные принципы управления ресурсами и организации доступа к этим ресурсам.	**Текущий контрольв форме:** - устного и письменного опроса; - тестирования; -написания рефератов, сообщений; - выполнения заданий моделирования; **Рубежный контроль** по каждому разделу в форме устного опроса **Форма промежуточной аттестации** - экзамен