МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
СМОЛЕНСКИЙ КАЗАЧИЙ ИНСТИТУТ ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И БИЗНЕСА (ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»
(СКИПТБ (ФИЛИАЛ) ФГБОУ ВО «МГУТУ ИМ. К. Г. РАЗУМОВСКОГО (ПКУ)»)

УТВЕРЖДАЮ
Директор СКИПТБ (филиал) ФГБОУ ВО
«МГУТУ им. К.Г. Разумовского (ПКУ)
_____ Н.С. Коржикова
«28» июня 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ 02. ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

профессионального учебного цикла
программы подготовки специалистов среднего звена

по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

уровень подготовки
базовый

Квалификация
Техник по защите информации

форма обучения
очная

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00B895E5D3E87E5E81C0F723DE8AC92877
Владелец: Коржикова Надежда Сергеевна
Действителен: с 06.08.2024 до 30.10.2025

Вязьма 2023

ОДОБРЕНА
предметной (цикловой) комиссией
общепрофессиональных дисциплин,
профессиональных модулей специальности
10.02.05 «Обеспечение информационной
безопасности автоматизированных систем»
Председатель ПЦК

_____А.А. Иванов

Протокол № 10 от «26» июня 2023 г.

СОГЛАСОВАНО

Заместитель директора

_____О.В. Комарова

«26» июня 2023 г.

Составитель (автор):
Преподаватель без
квалификационной категории _____А.А. Иванов

Рабочая программа рекомендована к утверждению экспертами:
Генеральный директор
ООО «Споит» _____Н.В. Савин
(М.П.)

Специалист по защите
информации ФГКУ комбинат
«Прожектор» Росрезерва» _____Н.В. Готовщикова

Рабочая программа разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности **10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**, утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 № 1553, и учебного плана программы подготовки специалистов среднего звена по специальности **10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**

СОДЕРЖАНИЕ

1	ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2	СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ	7
3	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	10
4	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ	12
5	ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	13

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Цель и планируемые результаты учебной практики

В результате прохождения практики профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, студент должен освоить вид деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.1.2. 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.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	- установки, настройки программных средств защиты информации в автоматизированной системе; - тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; - учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности.
уметь	- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; - 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.
знать	- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; - 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.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

Коды профессиональных компетенций	Наименования разделов практики	Количество часов		
		Учебная практика	Производственная практика (по профилю специальности)	Преддипломная практика
1	2	3	4	5
ПК 2.1, ПК 2.2 ПК 2.3, ПК 2.4, ПК 2.5 ПК 2.6	УП.02.01 Программные и программно-аппаратные средства защиты информации	50	-	-
ПК 2.1, ПК 2.2 ПК 2.3, ПК 2.4, ПК 2.5 ПК 2.6	УП.02.02 Криптографические средства защиты информации	22		
	Всего:	72	-	-

3.2. Содержание учебной практики

Наименование разделов и тем	Виды выполняемых работ	Объем часов
1	2	3
УП.02.01. Программные и программно-аппаратные средства защиты информации.		**50**
Введение.	**Виды выполняемых работ**	**2**
	Введение в учебную практику. Цели и задачи учебной практики. Техника безопасности.	2
Раздел 1. Использование программно-аппаратной защиты обеспечения безопасности информационных систем.	**Виды выполняемых работ**	**8**
	Тема 1.1. Методы использования парольной защиты. Практическая работа № 1. Разработка схемы простого пароля.	2
	Практическая работа № 2. Количественная оценка стойкости парольной защиты.	2
	Практическая работа № 3. Разработка парольных подсистем на базе простейшего генератора паролей.	2
	Практическая работа № 4. Разработка динамически изменяющегося пароля.	2
	Виды выполняемых работ	**40**
	Тема 1.2. Виртуальные машины как средство защиты автоматизированных информационных систем. Практическая работа № 5. Установка платформы виртуализации Oracle VirtualBox.	2
	Практическая работа № 6. Установка гостевой ОС CentOS. Настройка локальных параметров.	2
	Практическая работа № 7. Управление и работа с пользователями в ОС CentOS с помощью командной строки.	2
	Практическая работа № 8. Работа с процессами в ОС CentOS.	2
	Практическая работа № 9. Управление процессами в ОС CentOS.	2
	Практическая работа № 10. Подсистема регистрации событий в ОС CentOS.	2
	Практическая работа № 11. Мониторинг и аудит информационной безопасности на основе анализа системных журналов и журналов событий в ОС.	2
	Практическая работа № 12. Распределение прав доступа и управление пользователями и группа посредством графического интерфейса KDE.	2
	Практическая работа № 13. Разграничение прав доступа в ОС CentOS.	2
	Практическая работа № 14. Работа со служебными программами KDE CentOS. Мониторинг и удаление остаточной информации.	2
	Практическая работа № 15. Создание сертификатов электронной подписи.	2
	Практическая работа № 16. Шифрование файловой системы**.**	2
	Практическая работа № 17. Исследование защиты виртуальной машины от внешнего воздействия. Настройка межсетевого экрана с помощью IPTABLES.	2

	Практическая работа № 18. Создание замка защиты программы от несанкционированного использования.	2
	Тема 1.3. Программно-аппаратные средства обеспечения безопасности информационных систем. Практическая работа № 19. Исследование характеристик систем АМДЗ "Аккорд", МДЗ "Электронный замок "Соболь", АПМДЗ семейства "Криптон-Замок".	4
	Практическая работа № 20. Исследование электронного замка "Соболь".	2
	Практическая работа № 21. Исследование характеристик систем "StrongDisk" и "SecretDisk".	2
	Практическая работа № 22. Программное средство КЗИ "Верба".	2
	Практическая работа № 23. Исследование конструктивных и технических особенностей систем "Dallas Lock" и "Secret Net".	2
УП.02.02. Криптографические средства защиты информации.		**22**
Раздел 2. Криптографические средства защиты информации.	**Виды выполняемых работ**	**22**
	Тема 2.1. Криптографические средства защиты информации. Криптографическая защита информации.	2
	Практическая работа № 24. Реализация шифра безключевого и ключевого шифра перестановки и его криптоанализ.	4
	Практическая работа № 25. Реализация ранцевой криптосистемы.	4
	Практическая работа № 26. Реализация шифра "одноразовый блокнот" и его криптоанализ.	4
	Практическая работа № 27. Шифрование данных по ГОСТ 28147-89.	4
	Практическая работа № 28. Реализация алгоритма шифрования по схеме Эль Гамаля.	2
	Практическая работа № 29. Реализация алгоритма шифрования RC4.	2
Всего		**72**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

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

Реализация программы дисциплины требует наличия учебного кабинета информационной безопасности, лаборатории информационных технологий.

Оборудование учебного кабинета: персональный компьютер, проектор, презентации уроков, стенды, плакаты, методические пособия.

Оборудование лаборатории информационных технологий: посадочные места по количеству обучающихся; рабочее место преподавателя; мультимедийное оборудование.

3.2. Информационное обеспечение реализации программа

Для реализации программы библиотечный фонд образовательной организации для использования в образовательном процессе должен иметь печатные и/или электронные образовательные и информационные ресурсы.

3.2.1. Печатные издания

Основные печатные источники

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования 2-е издание. - М.: Издательский центр «Академия», 2016.

Дополнительные печатные источники:

1. Башлы П.Н., Бабаш А.В., Баранова Е.К. Информационная безопасность и защита информации [Электронный ресурс] : Учебник. - М: РИОР, 2013. – Режим доступа: http://znanium.com/
2. Белов Е.Б. и др. Основы информационной безопасности : учеб. пособие для студентов вузов. - М: Горячая линия - Телеком, 2006.
3. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах (Среднее профессиональное образование) - М: Форум, 2009.
4. Гарнаев А.Ю. Самоучитель VBA. СПб.: БВХ, 2009.
5. Канцедал С.А. Алгоритмизация и программирование : учебное пособие. - М: ФОРУМ, 2010.
6. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации : учеб. пособие для студентов вузов / под ред. С.А. Клейменова. - М: Академия, 2013.
7. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие (Профессиональное образование). - М: ФОРУМ: ИНФРА-М, 2012.

3.2.2. Электронные источники

1. Единый портал доступа к информационным образовательным ресурсам http://window.edu.ru
2. Сайт Научной электронной библиотеки www.elibrary.ru
3. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
4. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
5. Федеральный портал «Российское образование» www.edu.ru
6. Федеральный центр образовательных ресурсов http://fcior.edu.ru
7. Партыка Т.Л., Попов И.И. Информационная безопасность : учеб. пособие для студ. учреждений среднего проф. образования. [Электронный ресурс] - М.: ИД «ФОРУМ»: ИНФРА-М, 2016. Режим доступа: http://znanium.com/bookread2.php?book=915902
8. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. [Электронный ресурс] - М: Форум, 2016. – Режим доступа: http:// znanium.com/bookread2.php?book=537054/

3.2.3. Периодические издания

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал.
3. Информационная безопасность регионов: Научно-практический журнал.
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	- оценка выполнения практических работ; - оценка качества сформированных знаний студента при проведении устного опроса.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	

Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			
3.			
4.			