Приложение № 4
к образовательной программе среднего профессионального образования – программе подготовки специалистов среднего звена по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (на базе основного общего образования)

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «НАУЧНО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «СИРИУС»
(АНОО ВО «УНИВЕРСИТЕТ «СИРИУС»)

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты»

1. Трудоемкость профессионального модуля: 378 ак.ч.

2. Место профессионального модуля в учебном плане:

Профессиональный модуль «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты» входит в образовательный компонент программы П.00 «Профессиональный цикл» (ПМ.02) и является обязательным. Профессиональный модуль реализуется в 4-7 семестрах.

3. Цель профессионального модуля: формирование теоретических знаний и практических навыков в области защиты информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты.

4. Задачи профессионального модуля:

- познакомить студентов с современными программно-аппаратными средствами защиты информации в компьютерных системах и обучить методам решения задач программно-аппаратной защиты информации;
- сформировать фундаментальные знания основных положений теории криптографической защиты информации, принципов построения симметричных и асимметричных шифров, схем цифровой подписи и функции хеширования, инфраструктуры систем управления ключами, оценки криптостойкости, имитостойкости и помехоустойчивости шифров, криптографических протоколов;
- познакомить с рисками использования средств виртуализации, научить методам защиты средств виртуализации и виртуальных систем;
- познакомить студентов с основными проблемами и способами обеспечения безопасности систем баз данных, научить методам корректного администрирования и настройки СУБД включая вопросы резервирования и репликации БД.

5. Перечень разделов (тем) профессионального модуля и их краткое содержание:

Наименования разделов (тем) профессионального модуля	**Содержание разделов (тем) профессионального модуля**
МДК.02.01 «Программные и программно-аппаратные средства защиты информации»	
Раздел 1. Разработка политики информационной безопасности компьютерной системы.	Разработка политики информационной безопасности. Методология политики безопасности компьютерных систем. Основные положения политики информационной безопасности. Жизненный цикл политики безопасности. Принципы политики безопасности.
Раздел 2. Разработка модели угроз компьютерной системы.	Объекты угроз. Классификация угроз по способу их осуществления. Классификация объектов угроз. Функциональная модель системы защиты. Состав и назначение функциональных блоков. Основные группы механизмов защиты. Функциональная модель. Рекомендации по отдельным уровням функциональной модели. Дискреционные и мандатные модели.

Раздел 3. Идентификация и аутентификация.	Основные понятия и классификация. Простая аутентификация. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе сертификатов. Биометрическая идентификация и аутентификация пользователей. Строгая аутентификация. Протоколы аутентификации с симметричными алгоритмами шифрования. Протоколы, основанные на использовании однонаправленных ключевых хэш - функций. Аутентификация с использованием асимметричных алгоритмов шифрования. Аутентификация, основанная на использовании цифровой подписи. Протоколы аутентификации с нулевой передачей значений. Упрощенная схема аутентификации с нулевой передачей знаний. Параллельная схема аутентификации с нулевой передачей знаний.
Раздел 4. Замкнутая программная среда	Система защиты информации от несанкционированного доступа «СТРАЖ NT». Установка и снятие СЗИ. Управление пользователями. Учет носителей и контроль устройств.
Раздел 5. Защита файловой системы Windows	Разрешения для файлов и папок. Шифрующая файловая система (EFS) Encrypting File System. Технология шифрования. Восстановление данных. Процесс шифрования. Процесс дешифрирования. Процесс восстановления. Взаимодействие файловой системы защиты NTFS и защиты ресурса общего доступа (Sharing). Типовые задачи администрирования. Администрирование дисков в Windows. Сходства и различия между Disk Management и Disk Administrator.
Раздел 6. Защита файловой системы OS Linux.	12. Файловая система OS Linux. Основные концепции файловой системы. Виртуальная Файловая Система (VFS). Файловые системы EXT2 (The Second Extended File System) шифрования. Процесс дешифрирования. Процесс восстановления. Взаимодействие файловой системы защиты NTFS и защиты ресурса общего доступа (Sharing). Типовые задачи администрирования. Администрирование дисков в Windows. Сходства и различия между Disk Management и Disk Administrator. Шифрующая файловая система (EFS) Encrypting File System.
Раздел 7. Программно-аппаратные комплексы VipNet	Принцип функционирования защищенной сети ViPNet. Архитектура ViPNet Administrator 4.x. Модификация защищенной сети и настройка политик безопасности на узлах. Модификация защищенной сети и настройка политик безопасности на узлах. Установка программного комплекса ViPNet Administrator. Работа с ViPNet Coordinator for Windows. ViPNetClient.
МДК.02.02 «Криптографические методы защиты информации»	
Раздел 1. Основные понятия криптографии	Модели шифров. Классификация методов криптографической защиты информации. Простейшие шифры подстановки и их свойства. Шифры перестановки их свойства. Блочный шифр. Ключевая система.

Раздел 2. Алгоритм шифрования	Алгоритм шифрования таблицей Виженера. Американский стандарт шифрования DES. Шифрование алгоритмом S-DES. Расшифрование алгоритмом S-DES. Стандарт криптографической защиты AES. Принципы работы алгоритма шифрования AES. Шифрование алгоритмом S-AES. Стандарт шифрования данных Магма. Шифрование и расшифрование алгоритмом S-Магма. 18. Отечественный стандарт шифрования «Кузнечик».
Раздел 3. Электронная цифровая подпись	Построение электронной цифровой подписи RSA. Практическая реализация электронных цифровых подписей. Построение электронной цифровой подписи Эль-Гамаля. Управление ключами. Ключевой обмен на основе алгоритма Диффи-Хеллмана. Модифицированный метод ключевого обмена на основе алгоритма Диффи-Хеллмана.
Раздел 4. Протоколы аутентификации	Протокол аутентификации Шнорра. Протоколы аутентификации с нулевым разглашением знаний и их применение. Протокол аутентификации для систем электронных платежей. Криптографические хеш-функции. Отечественная криптографическая хеш-функция.
МДК.02.03 «Защита ИТ-систем»	
Раздел 1. Особенности уровней L3-4, L7	Углубленное изучение модели OSI. Особенности сетевого и транспортного уровня. Прикладной уровень - угрозы современности.
Раздел 2. DDoS-атаки, их разновидности, методы обнаружения и отражения	Наиболее распространенные типы DDoS-атак на уровнях L3 и L4; IP fragmented flood. ICMP flood. TCP flood. SYN flood. UDP flood. Методы обнаружения и защиты от DDoS-атак.
Раздел 3. Системы анализа трафика.	DNS amplification, как разновидность DDoS на уровне L7. HTTP-флуд. SQL-инъекции. XSS-атаки. DoS-атаки на специфические функции. Программно-аппаратные решения анализа трафика. NGFW – практика использования.
Раздел 4. Средства виртуализации и методы их защиты.	Жёсткая изоляция и сегментация. Обновление и патчинг гипервизоров. Использование минимизированных и проверенных образов.

	Мониторинг и аудит безопасности. Контроль доступа и аутентификация. Безопасность сетевого взаимодействия.
Раздел 5. Типы средств защиты систем виртуализации	Использование универсальных средств защиты для обеспечения безопасности виртуальных систем. Специализированные средства защиты для виртуализации.
Раздел 6. Российские средства защиты систем виртуализации.	Практика использования и сравнение систем: vGate 5.0 и Dallas lock ВИ.
Раздел 7. Особенности систем БД как объекта защиты	Угрозы безопасности БД. Администрирование СУБД.
Раздел 8. Управление доступом. Учетные записи. Аутентификация. Управление привилегиями.	Модели управления доступом. Учетные записи и аутентификация в разных СУБД. Привилегии в разных СУБД.
Раздел 9. Резервное копирование. Репликация и балансировка нагрузки. Секционирование и сегментирование.	Типы и классификация резервного копирования. Факторы планирования резервного копирования. Стратегии резервного копирования. Понятие, типы и виды топологии репликации.
Раздел 10. Аудит и мониторинг.	Задачи проблемы и методы аудита. Плагины аудита. Мониторинг хранилища данных.
Раздел 11. Шифрование, виды шифрования в системах БД.	Виды и риски шифрования в БД. Шифрование подвижных данных. Особенности шифрования в различных СУБД.
Раздел 12. SQL-инъекции	Основные понятия. Типы инъекций. Противодействие инъекциям.
Раздел 13. Целостность данных и транзакции.	Основные понятия целостности данных. Свойства транзакций и блокировки. Проблемы совместного доступа к данным. Уровни изоляции транзакций. MVCC.
Раздел 14. Защита данных встроенными средствами СУБД.	Представления. Хранимые процедуры и функции. Триггеры.
Раздел 15. Требования безопасности информации,	Необходимые организационные меры. Нормативные документы регуляторов. Сертифицированные ОС.

предъявляемые к ОС.	
Раздел 16. Способы обеспечения безопасности ОС.	Аутентификация и управление доступом. Диагностика и восстановление. Журналирование файловых систем. Протоколирование и аудит. Криптографическая защита. Гарантированное уничтожение информации.
Раздел 17. Особенности защиты в различных ОС.	Система безопасности ОС Windows. Защита в ОС UNUX. Безопасность виртуальных ОС. Безопасность ОС мобильных устройств.
УП.02.01 Учебная практика (Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты)	
Выполнение практических заданий по темам, изученным в МДК профессионального модуля. Закрепление освоенных навыков на учебных примерах	

6. Образовательные результаты освоения дисциплины (модуля):

Код и наименование компетенции	Результаты освоения дисциплины
ЛК-02. Использует современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	ИЛК-02.3. Организует собственную деятельность для решения стандартных профессиональных задач, действуя в рамках целей и способов, определенных руководителем
ЛК-05. Осуществляет устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	ИЛК-05.3. Грамотно излагает свои мысли и оформляет документы по профессиональной тематике на государственном языке
ПК-01. Выполняет монтаж, настройку и администрирование сетевого оборудования и систем обеспечения информационной безопасности	ИПК-01.4. Реализует сетевую безопасность (межсетевые экраны, VPN, ACL, IDS/IPS)
ПК-03. Применяет программно-аппаратные средства и методы обеспечения информационной безопасности, включая тестирование на проникновение и анализ защищённости	ИПК-03.1. Применяет криптографические средства и методы защиты информации
	ИПК-03.2. Способен устанавливать и конфигурировать программно-аппаратные средства защиты информации