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 ДИСЦИПЛИНЫ (МОДУЛЯ)

«Основы информационной безопасности (введение в профессию)»

1. Трудоемкость дисциплины (модуля): 72 ак.ч.

2. Место дисциплины (модуля) в учебном плане:

Дисциплина «Основы информационной безопасности (введение в профессию)» входит в образовательный компонент программы ОП.00 «Общепрофессиональный цикл» (ОП.09) и является обязательной. Дисциплина реализуется в 1-2 семестрах.

3. Цель дисциплины (модуля): формирование у обучающихся начальных знаний и навыков в области информационной безопасности, направленных на осознание важности защиты информации, умение выявлять возможные угрозы и предпринимать базовые меры по предотвращению несанкционированного доступа, утечки данных и иных нарушений конфиденциальности, целостности и доступности информации.

4. Задачи дисциплины (модуля):

- познакомить с основными понятиями и терминологией информационной безопасности: определение угроз, уязвимостей, рисков, средств защиты и методов обеспечения безопасности;
- развить понимания природы угроз и источников опасности: изучение факторов, влияющих на возникновение угроз информационной безопасности, и путей их преодоления;
- способствовать приобретению навыков анализа и оценки рисков: ознакомление с методиками выявления потенциальных угроз и уязвимостей, способами оценки степени риска и необходимостью защитных мер;
- познакомить на практике с мерами защиты информации: изучение и применение базовых методов и средств защиты, таких как парольные политики, шифрование, ограничение прав доступа и прочие;
- сформировать представления о правовых аспектах информационной безопасности: ознакомление с действующими законодательствами, международными нормами и правилами, регулирующими обработку и защиту информации;
- подготовить к дальнейшей специализации в области информационной безопасности: закрепление интереса к профессии и получение первичных знаний, необходимых для углубленного изучения отдельных аспектов информационной безопасности в последующих курсах.

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

Наименования разделов (тем) дисциплины (модуля):	Содержание разделов (тем) дисциплины (модуля):
Раздел 1. Основные понятия и определения информационной безопасности	1. Терминология информационной безопасности (ИБ): угрозы, риски, атаки, уязвимости, защитные меры. 2. Цель и задачи информационной безопасности: конфиденциальность, целостность, доступность (триада CIA). 3. Нормативно-правовая база регулирования ИБ в России (Федеральный закон №152-ФЗ, ГОСТы, приказы ФСБ и ФСТЭК).
Раздел 2. Источники и природа угроз информационной безопасности	5. Внешние и внутренние угрозы: хакеры, инсайдеры, вредоносное ПО, DoS/DDoS-атаки. 6. Причины возникновения угроз: человеческие

	факторы, ошибки разработчиков, недостаточная осведомленность пользователей. 7. Методы выявления и оценки угроз (анализ угроз, инвентаризация активов, Risk Assessment).
Раздел 3. Методы и средства защиты информации	9. Шифрование и криптографические методы защиты (симметричные и асимметричные алгоритмы, хеширование). 10. Биометрические системы и методы аутентификации (пароли, токены, отпечатки пальцев, распознавание лиц). 11. Средства ограничения доступа и управления правами (контроллеры доменов, списки ACL, группы пользователей).
Раздел 4. Атаки и контрмеры	13. Виды кибератак: социальная инженерия, вирусы, черви, троянские программы, фишинг, спуфинг. 14. Современные методы защиты от кибератак: антивирусные программы, firewalls, Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS). 15. Ответственность за нарушения информационной безопасности и юридические последствия неправомерных действий.
Раздел 5. Безопасность сети и телекоммуникационной инфраструктуры	17. Безопасность локальных и глобальных сетей (защита маршрутизаторов, шлюзов, DNS, VPN). 18. Защищенность беспроводных сетей (Wi-Fi, Bluetooth, NFC). 19. Основы сетевой безопасности и способы её укрепления (фильтрация пакетов, сегментация сети, NAT, VPN).
Раздел 6. Безопасность веб-приложений и облачной инфраструктуры	21. Типичные уязвимости веб-приложений (SQL-инъекции, XSS, CSRF, XXE). 22. Принципы безопасной разработки веб-приложений (OWASP Top Ten, SDLC). 23. Безопасность облачных сервисов (Public Cloud, Private Cloud, Hybrid Cloud).
Раздел 7. Политики и процедуры информационной безопасности	25. Разработка и внедрение политики информационной безопасности в организации. 26. Регламентирующие документы и положения по управлению рисками (матрицы рисков, карта угроз). 27. Внутренняя проверка соблюдения норм информационной безопасности (internal audit).
Раздел 8. Этический хакинг и тесты на проникновение	29. Понятия этичного взлома (ethical hacking) и его отличия от преступных действий. 30. Этапы проведения тестов на проникновение (penetration testing): разведка, сканирование, атака, отчётность. 31. Ограничения и ответственность тестировщиков в

	ходе испытаний на проникновение.
Раздел 9. Будущие тенденции и новые вызовы в информационной безопасности	33. Тенденции и прогнозы развития ИБ: рост числа кибератак, развитие AI и ML в ИБ, биометрия, квантовая криптография. 34. Новые вызовы и угрозы информационной безопасности (автоматизация атак, краудсорсинг атак, атаки с применением искусственного интеллекта).

6. Образовательные результаты освоения дисциплины (модуля):

Код и наименование компетенции	Результаты освоения дисциплины
ЛК-01. Выбирает способы решения задач профессиональной деятельности применительно к различным контекстам	ИЛК-01.5. Реализует составленный план, эффективно выполняя несколько разноплановых профессиональных задач без потери качества
	ИЛК-01.6. Оценивает результат решения задачи и последствия своих действий (самостоятельно или с помощью наставника), применяя установленный порядок оценки результатов профессиональной деятельности
ПК-03. Применяет программно-аппаратные средства и методы обеспечения информационной безопасности, включая тестирование на проникновение и анализ защищённости	ИПК-03.2. Способен устанавливать и конфигурировать программно-аппаратные средства защиты информации