Приложение № 4
к образовательной программе среднего профессионального образования -
программе подготовки специалистов среднего звена
по специальности 09.02.06 Сетевое и системное администрирование

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

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«Основы сетевой и информационной безопасности»

1. Трудоемкость профессионального модуля: 288 ак.ч.

2. Место профессионального модуля в учебном плане:

Профессиональный модуль «Основы сетевой и информационной безопасности» входит в образовательный компонент программы П.00 «Профессиональный цикл» (ПМ.06) и является вариативным. Профессиональный модуль реализуется в 3-6 семестрах.

3. Цель профессионального модуля: формирование компетенций по обеспечению безопасного и эффективного функционирования ИТ-инфраструктуры посредством применения знаний и практических навыков, необходимых для выявления, анализа и устранения уязвимостей в системах, а также разработки стратегии по защите информации от различных угроз.

4. Задачи профессионального модуля:

– сформировать знание принципов выстраивания инфраструктуры безопасности организации;

– сформировать знания и представления о различных типах угроз и уязвимостей, с которыми могут столкнуться информационные системы, а также методах их обнаружения и оценки;

– приобретение умений и навыков по работе с межсетевыми экранами, системами обнаружения и предотвращения вторжений криптографическими средствами и другими современными технологиями, которые обеспечивают защиту данных;

– изучить принципы выстраивания архитектуры SOC;

– сформировать навыки по конфигурированию операционных систем для обеспечения информационной безопасности;

– сформировать навыки применения методов Incident Response и AAA (Authentication, Authorization, Audit).

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

Наименования разделов (тем) профессионального модуля	Содержание разделов (тем) профессионального модуля
МДК.06.01 Основы сетевой и информационной безопасности	
Раздел 1. Актуальные задачи информационной безопасности	Классификация злоумышленников, уязвимостей и атак. Примеры уязвимостей и атак. Мотивация злоумышленников как цели для атак. Цели по защите компаний: снижение финансового риска - невозможность кражи денежных средства, снижение риска утечки данных компании / репутационные риски, бесперебойность предоставляемого сервиса, снижение влияния на сервис из-за кибератак и внутреннего злоумышленника. Влияние кибератак на на жизнь людей. Основные концепции ИБ: целостность - свойство сохранения правильности и полноты активов; доступность - возможность получения информации/сервиса и её использования, конфиденциальность - необходимость предотвращения разглашения информации. Основные векторы первичной компрометации систем: социальная инженерия, сервисы

	удалённой работы/периметр, Misconfiguration / Vulnerability, DDoS Attacks, Supply Chain Attacks / watering hole. Основные типы вредоносных программ. Современные вызовы и организация информационной безопасности в компаниях: человеческий фактор, ускорение технологий, кибертерроризм, уход экспертизы и альтернативного мнения. Основные направления ИБ: Infrastructure Security, Infrastructure Security, Data security, Security Operations, Cryptography, Compliance, Governance, Research & development, Awareness. Обзор и анализ компетенции необходимые для специалистов по ИБ.
Раздел 2. Защита ОС	Linux Security: обзор ОС – ядро, основные команды, файловая система, права доступа. Протокол SSH – установка клиента и сервера, методы защиты SSH, блокировка пароль root, замена стандартного порта SSH, запрет авторизации по паролю, Ограничение IP-адресов, с которых возможен доступ, Fail2ban для защиты SSH, конфигурация Fail2ban, параметры политики паролей, Iptables Process Flow, синтаксис утилиты iptables, действия с соединениями, критерии для пакетов, примеры команд, анализ открытых портов при помощи netstat, основные лог файлы, аудит системных событий в Linux, создание правил. Windows Security: ядро, основные команды, файловая система, права доступа. Параметры политик безопасности, примеры команд, анализ открытых портов, основные лог-файлы, аудит системных событий, создание правил. Составляющие критичности: критичные данные - персональные данные, платежные данные, аутентификационные данные; тайна (банковская, государственная, коммерческая, связи, медицинская); Критичные действия – блокировка, управление бонусами и акциями, сброс/замена/перенос (пароля, токена, SIM/банковской карты, второго фактора, кодового слова), дубликация/дедубликация клинета/абонента; проведение платежей; аудиты, регуляторные требования; публикация в интернет; внешние интеграции; критичные интеграции; большое число пользователей. Подключение других команд ИБ: на базе типов данных, на базе процессов, в связи с отраслью компании. Минимизация поверхности атаки: на сетевом уровне - сетевая сегментация, запрещенные порты, протоколы, VPN, сокращение периметра; на уровне компонентов приложения – аутентификация, роли/группы доступа,

	Secure in transit; на уровне приложения – минимизация предоставляемых/запрашиваемых данных.
Раздел 3. Анализ проектов с точки зрения безопасности	Основные термины. Что такое критичность? Соответствие стандартам vs управление риском. Анализ проекта: определение критичности, сбор информации, подключение команд ИБ, применимые угрозы, требования и контроли, остаточные риски. Моделирование угроз. Подходы при создании модели угроз: Asset-Centric (проще обосновать бизнесу, более интуитивный при коммуникации с другими подразделениями), Attacker-Centric (более интуитивный при взаимодействии внутри ИБ), Software-Centric (базируется на моделях производителей ПО, упрощает коммуникацию с ИТ и разработчиками). Методики выявления угроз: SABSA, Security Boundary, Оценка риска (DREAD) и т.д. Модель злоумышленника. Примеры акторов
МДК.06.02 Основы криптографии для защиты информации	
Раздел 1. Безопасность сетей	Обзор модели OSI и топологий. Разновидности FireWall: управляемые коммутаторы, пакетные фильтры, шлюзы сеансового уровня, инспектор состояния, посредники прикладного уровня. Обзор протоколов по степени их защищённости. Сегментация сети как средство повышения безопасности. Концепция Zero-trust: в центре защиты – данные, нет доверенной зоны, шифрование всего траффика, аутентификация /авторизация всех компонентов, жесткое управление сетью. Объединение сетей: VPN, IPSec. Инструменты защиты: Intrusion detection system, Intrusion prevention system, NGFW, UTM, Honeypot. Атаки на корпоративные сети: пассивные действия - общий поиск, гугглинг, DNS, сниффинг траффика; активные действия - сканирование портов, сканирование, Smurfing, Smuggling, DNS poisoning, MITM

Раздел 2. Контроль доступа	Аутентификация, авторизация, PoLP, RBAC, ABAC, Oauth 2.0, SECCOMP. Отличия процессов: аутентификация - процесс проверки подлинности, «пользователь действительно тот, кем представляется»; авторизация - процесс предоставления прав на выполнение определенных действий, с последующей проверкой на наличие таких прав. Принцип наименьших привилегий (PoLP): только необходимые данные - усложнение поиска вектора, увеличение его длины, усложнение бокового перемещения и повышение привилегий; только необходимые действия - усложнение поиска вектора атаки, усложнение бокового перемещение и повышение привилегий; только в конкретное время - замедление злоумышленника. Граница безопасности – множество интерфейсов между доверенной вычислительной средой (TCB) и остальным окружением. Граница безопасности – граница между компонентами, имеющими общие интерфейсы, но различные требования и политики безопасности. Граница доверия – виртуальная граница, в которой среда выполнения или данные меняют свой уровень доверия (привилегии). SECCOMP – Secure computing mode, назначение - изоляция процесса для обработки пользовательских данных.
Раздел 3. Incident Response. Архитектура SOC	Что является алертом – аномалия, конкретное оповещение. Что является инцидентом – действия злоумышленника, ошибки пользователя, сбой системы, нарушение требований. Процессы Incident Response: Preparation, Identification, Containment, Eradication, Recovery, Post-Incident Activity. Инструменты Incident Response: Kansa, Live Response Collection, Forensic Tool Kit, DD, Belkasoft RAM capturer, PowerShell, Iptables, СЗИ, физическое отключение. Политика аудита Windows: SecPol, gpedit.msc, логирование PowerShell, локальная политика аудита, расширенная политика аудита. Логирование командных строк. SACL. Детектирование mimikatz.
МДК.06.03 Квантовая криптографии	
Раздел 1. Угрозы квантовых компьютеров для классических криптосистем	Асимметричная криптография. Симметричная криптография. Концепция «Собери сейчас, расшифруй потом»
Раздел 2. Принципы квантового распределения ключей (QKD) на основе протокола BB84	Идея протокола BB84 (Беннет и Брассар, 1984). Пошаговая процедура (без погружения в физику).

Раздел 3. Состав оборудования и среда передачи данных в системах QKD	Аппаратные компоненты. Среда передачи. Физические ограничения.
Раздел 4. Практические сценарии применения QKD в отраслях экономики и государственном управлении	Финансовый сектор (Банки, биржи). Государственное управление и оборона. Энергетика и Критическая инфраструктура.
Раздел 5. Сравнительный анализ квантового распределения ключей (QKD) и постквантовой криптографии (PQC)	Постквантовая криптография (PQC) — математический подход. QKD — физический подход. Синтез (Гибридный подход).
УП.06.01 Учебная практика (Основы сетевой и информационной безопасности)	
Выполнение практических заданий по темам, изученным в МДК профессионального модуля. Закрепление освоенных навыков на учебных примерах	

6. Образовательные результаты освоения профессионального модуля:

Код и наименование компетенции	**Результаты освоения профессионального модуля**
ПК-14. Обеспечивает защиту информации в сети при помощи специальных программно-аппаратных средств	ИПК-14.1 Обеспечивает конфиденциальность и безопасность при работе в Интернете
	ИПК-14.2 Применяет специальные устройства и ПО для обнаружения уязвимостей ИС и сетей
	ИПК-14.3 Применяет специальные устройства и ПО для защиты ИС и сетей
	ИПК-14.4 Знает и применяет протоколы и методы концепции AAA