Приложение № 4
к образовательной программе высшего образования – программе магистратуры
по направлению подготовки 09.04.01 Информатика и вычислительная техника
(направленность (профиль) «Разработка и управление
критической информационной инфраструктурой»)

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 7835bcdac1c89a3da835a18f6045494f3f404337
Владелец: Некрасова Людмила Андреевна
Действителен: с 08.07.2026 до 08.07.2027

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«Проектирование и разработка защищенных информационных систем»

1. Трудоемкость дисциплины (модуля): 4 з.е.

2. Место дисциплины (модуля) в учебном плане:

Обязательная часть «Профессиональной подготовки» в рамках Блока 1. Дисциплины (модули), реализуется в 3 семестре.

3. Цель дисциплины (модуля): изучение методов проектирования и реализации защищенных информационных систем; знакомство с принципами и методами обеспечения безопасности информационных систем и защиты информации, включая криптографические методы и управление ключами; формирование навыков проектирования и настройки механизмов аутентификации, обнаружения и предотвращения вторжений.

4. Задачи дисциплины (модуля):

– сформировать представление о принципах, моделях и архитектурах построения защищенных информационных систем и о современных угрозах их безопасности;

– обеспечить владение методами и инструментами проектирования механизмов аутентификации, разграничения доступа и криптографической защиты данных;

– научить разрабатывать, настраивать и оценивать защищенность информационных систем, включая средства обнаружения и предотвращения вторжений.

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

Наименование раздела (темы) дисциплины (модуля)	**Краткое содержание**
Раздел 1. Принципы и модели построения защищенных информационных систем	Понятие защищенной информационной системы. Угрозы и модель нарушителя. Политики и модели безопасности (дискреционная, мандатная, ролевая). Принципы проектирования: минимизация привилегий, эшелонированная защита, защита по умолчанию.
Раздел 2. Архитектура и жизненный цикл защищенной ИС	Этапы жизненного цикла защищенной ИС. Формирование требований безопасности. Архитектурные решения и компоненты защиты. Безопасная разработка (SDL). Документирование и сопровождение.
Раздел 3. Аутентификация и управление доступом	Механизмы идентификации и аутентификации. Многофакторная аутентификации. Управление учетными записями и привилегиями. Модели и реализация разграничения доступа.
Раздел 4. Криптографические методы защиты и управление ключами	Симметричные и асимметричные алгоритмы. Хеширование и электронная подпись. Инфраструктура открытых ключей (PKI). Управление жизненным циклом ключей. Защита данных при хранении и передаче.

Наименование раздела (темы) дисциплины (модуля)	Краткое содержание
Раздел 5. Обнаружение и предотвращение вторжений	Системы обнаружения и предотвращения вторжений (IDS/IPS). Сетевые и хостовые средства защиты. Мониторинг событий безопасности. Реагирование на инциденты.
Раздел 6. Оценка защищенности и сопровождение системы	Методы оценки защищенности. Тестирование на проникновение. Аудит безопасности. Соответствие нормативным требованиям и стандартам. Сопровождение и обновление средств защиты.

6. Образовательные результаты освоения дисциплины (модуля):

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ПК-1. Способен создавать защищенные информационные системы с использованием криптографических методов	ИПК-1.1. Владеет основами криптографии, современными методами защиты информации, технологиями создания информационных систем
	ИПК-1.2. Умеет проектировать и разрабатывать отдельные элементы защищенных информационных систем с использованием криптографических методов
	ИПК-1.3. Владеет методами создания и внедрения информационных систем, а также обеспечивает их защиту с помощью криптографических методов
ПК-3. Способен анализировать и обеспечивать безопасность компьютерных сетей, включая распределенные, облачные и высоконагруженные системы	ИПК-3.1. Знает основные принципы компьютерной сетевой безопасности и методы анализа уязвимостей в локальных сетях и распределенных системах
	ИПК-3.2. Умеет исследовать компьютерные сети, распределенные, облачные и высоконагруженные системы, выявлять и устранять в них уязвимости
	ИПК-3.3. Владеет методами обеспечения безопасности компьютерных сетей, распределенных, облачных и высоконагруженных систем с помощью методов мониторинга и обнаружения инцидентов
ПК-6. Способен проектировать и реализовывать объекты критической информационной инфраструктуры для различных операционных систем и	ИПК-6.1. Знает принципы проектирования информационных систем и объектов критической инфраструктуры, особенности различных операционных систем и облачных платформ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
облачных платформ	ИПК-6.2. Умеет реализовывать объекты критической инфраструктуры для различных операционных систем и облачных платформ, учитывая их специфику
	ИПК-6.3. Владеет методами проектирования и реализации объектов критической инфраструктуры, включая установку, настройку и обеспечение их работоспособности с учетом специфики работы в различных операционных системах и облачных платформах