«Инновациялық Еуразия Университетінің Жоғары Екібастұз Колледжі» ЖШС

ТОО «Высший Экибастузский Колледж Инновационного Евразийского Университета»

|  |  |
| --- | --- |
| Информатика және техникалық пәндерінің  ЦӘК отырысында қарастырылды/  Рассмотрено на заседании ЦМК  Информатики и технических дисциплин  Хаттама/Протокол № \_\_\_\_  «\_\_\_»\_\_\_\_\_\_2024 ж./г.  \_\_\_\_\_\_\_\_\_\_\_\_\_Ахметова С.К. | Бекітемін / Утверждаю:  ОІЖ директор орынбасары/ зам. директора по УР  \_\_\_\_\_\_С.Я.Смагулова  «\_\_»\_\_\_\_\_\_\_\_\_2024ж/г |

МОДУЛЬ БОЙЫНША КУРСТЫҚ ЖОБАНЫ ОРЫНДАУҒА АРНАЛҒАН ӘДІСТЕМЕЛІК НҰСҚАУЛАР

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ВЫПОЛНЕНИЯ КУРСОВОГО

ПРОЕКТА ПО МОДУЛЮ

Мамандық/Специальность: 06120200 - Ақпараттық қауіпсіздік жүйелері/

06120200 -Системы информационной безопасности

Курс ІІІ

Семестр III

Тобы / Группа СИБ-322

Құрастырғандар/ Разработали:

\_\_\_\_\_\_\_\_Ахметова С.К.

\_\_\_\_\_\_\_\_\_Санатбек О.С.

Экибастуз, 2024

СОДЕРЖАНИЕ

|  |  |
| --- | --- |
| Пояснительная записка | 3 |
| Цели и задачи курсового проекта | 4 |
| Требования, предъявляемые к оформлению курсового проекта | 5 |
| Структура работы | 5 |
| Оформление работы | 10 |
| Тематика курсовых работ | 13 |
| Защита курсовой работы | 15 |
| Список рекомендуемой литературы | 16 |
| Примерный перечень вопросов для защиты курсовой работы | 17 |
| Образец титульного листа | 19 |

**Вступление:**

Облачные технологии стремительно развиваются, предлагая компаниям и частным лицам доступ к мощным вычислительным ресурсам, хранилищам данных и программному обеспечению по требованию. Однако с ростом популярности облачных сервисов возрастает и важность обеспечения их безопасности. В этой пояснительной записке мы рассмотрим основные аспекты безопасности облачных информационных инфраструктур.

**Цели проекта:**

**Изучение и анализ современных угроз безопасности облачных информационных инфраструктур:**

1. Определить основные типы угроз, их особенности и методы атак.
2. Проанализировать уязвимости, характерные для облачных сервисов, а также принципы их эксплуатации.

**Разработка комплексной модели обеспечения безопасности облачной инфраструктуры:**

1. Сформировать набор мер, позволяющих снизить уязвимость облачных решений и обеспечить безопасность данных и сервисов.
2. Определить роль и место различных механизмов безопасности в контексте облачной инфраструктуры.

**Практическая реализация модели обеспечения безопасности на конкретном примере:**

1. Продемонстрировать применение разработанных мер безопасности на конкретном облачном решении, например, Amazon Web Services (AWS) или Microsoft Azure.
2. Создать конфигурацию облачной инфраструктуры с учетом требований безопасности.

**Оценка эффективности разработанной модели:**

1. Провести анализ эффективности реализованной модели безопасности, оценить ее способность предотвращать угрозы и обеспечивать безопасность данных и сервисов.
2. Определить возможные улучшения и направления дальнейшего развития.

**Задачи проекта:**

1. **Обзор основных концепций безопасности в облаке:** Изучить модели безопасности, применимые к облачным инфраструктурам, такие как Shared Responsibility Model, Zero Trust, Security as Code.
2. **Анализ угроз безопасности облачных инфраструктур:** Изучить типичные виды угроз, такие как утечки данных, DDoS-атаки, phishing, malware attacks.
3. **Разработка модели безопасности облачной инфраструктуры:** Спроектировать систему безопасности, включающую физическую безопасность, сетевую безопасность, безопасность данных и приложений, управление доступом и аутентификацией.
4. **Выбор и конфигурирование средств обеспечения безопасности:** Определить подходящие средства безопасности для конкретной облачной инфраструктуры и настроить их в соответствии с разработанной моделью.
5. **Проведение тестирования модели безопасности:** Провести симуляцию атак и тестирование эффективности реализованных мер безопасности.
6. **Документация результатов:** Создать техническую документацию, описывающую модель безопасности, реализованные меры и результаты тестирования.

### 1. Обзор облачной информационной инфраструктуры

1.1 **Основные концепции облачных технологий**  
В этом подразделе будет рассмотрено, что такое облачные технологии, их основные характеристики и типы (IaaS, PaaS, SaaS). Обсудим, как облачные решения изменяют подходы к хранению и обработке данных.

1.2 **Преимущества и риски облачных решений**  
Здесь будет представлено сравнение преимуществ облачных технологий (гибкость, масштабируемость, экономия средств) и связанных с ними рисков, таких как утечка данных, зависимость от провайдеров и проблемы с соблюдением законодательства.

1.3 **Современные угрозы безопасности в облаке**  
Этот подраздел будет посвящён анализу текущих угроз, таких как атаки на уровень приложения, DDoS-атаки, несоответствие стандартам и уязвимости в настройках безопасности.

### 2. Анализ рисков и уязвимостей

2.1 **Актуальность исследования: методы сбора данных и инструменты**  
Здесь будет описан процесс сбора данных о безопасности облачных инфраструктур, включая опросы, интервью с экспертами и анализ существующих исследований. Также будет представлен обзор используемых инструментов.

2.2 **Визуализация и анализ данных: графики, диаграммы, таблицы**  
 В данном подразделе будет представлена визуализация собранных данных, включая графики и диаграммы, которые помогут проиллюстрировать выявленные уязвимости и риски.

2.3 **Идентификация ключевых угроз и уязвимостей: оценка рисков в области безопасности**  
Этот раздел сосредоточится на анализе собранных данных для выявления основных угроз и уязвимостей в облачной инфраструктуре. Будет проведена оценка рисков и предложены рекомендации по их минимизации.

### 3. Практическая часть

3.1 **Разработка и проектирование мер безопасности**  
В этом подразделе будет представлено проектирование комплекса мер безопасности, включающих шифрование данных, управление доступом, регулярное обновление систем и обучение сотрудников.

3.2 **Проведение практической реализации предложенных мер безопасности и тестирование их эффективности**  
Здесь будет описан процесс внедрения предложенных мер, включая тестирование их эффективности с помощью практических примеров и кейсов, а также анализ полученных результатов.

### Заключение

В заключении будет подведён итог исследования, обобщены ключевые выводы и предложены рекомендации по дальнейшему улучшению безопасности облачной информационной инфраструктуры.