**СИЛЛАБУС**

**Осенний семестр 2024-2025 учебного года**

Образовательная программа «6В07113 – Интеллектуальные системы управления»

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID и наименованиедисциплины** | **Самостоятельная работа обучающегося**  **(СРО)** | | **Кол-во кредитов** | | | **Общее**  **кол-во кредитов** | **Самостоятельная работа обучающегося**  **под руководством преподавателя (СРОП)** |
| **Лекции (Л)** | **Практ. занятия (ПЗ)** | **Лаб. занятия (ЛЗ)** |
| BVSS 4305 Безопасностьвычислительныхсистемисетей | 4 | | 1,7 | - | 1,6 | 3,3 | 6 |
| **АКАДЕМИЧЕСКАЯ ИНФОРМАЦИЯ О ДИСЦИПЛИНЕ** | | | | | | | |
| **Формат обучения** | **Цикл,**  **компонент** | **Типы лекций** | | **Типы практических занятий** | | **Форма и платформа**  **итогового контроля** | |
| *Офлайн* | М-16 IoT устройства и безопасность | Проблемный,  аналитический | | Выполнение лабораторной работы в среде Cisco packet tracer | | Устный экзамен (офлайн) | |
| **Лектор - (ы)** | Кунелбаев М.М. | | | | |
| **e-mail:** | murat7508@yandex.kz | | | | |
| **Телефон:** | +7(707)829-67-48 | | | | |
| **Ассистент- (ы)** | Cеребряков С. | | | | |
| **e-mail:** |  | | | | |
| **Телефон:** | +7(778)292-20-38 | | | | |
| **АКАДЕМИЧЕСКАЯ ПРЕЗЕНТАЦИЯ ДИСЦИПЛИНЫ** | | | | | | | |
| **Цель дисциплины** | **Ожидаемые результаты обучения (РО)\***  : | | | | | **Индикаторы достижения РО (ИД)** | |
| Цель дисциплины состоит в освоении базовых знаний и навыков, охватывающих все области информационной безопасности, безопасности систем и сетей, технологии и методы защиты. | 1. Понимание информационной безопасности. | | | | | Может объяснить основные принципы информационной безопасности. | |
| Приводит примеры компьютерных преступлений и классифицировать их по типам и идентифицируют основные угрозы безопасности информации. | |
| 2. Знание пользователей и злоумышленников в Интернете. | | | | | Может описать различные категории пользователей и их мотивацию в сети Интернет. | |
| Анализирует потенциальные угрозы безопасности, связанные с действиями злоумышленников. | |
| 3. Умение защищать от компьютерных вирусов. | | | | | Определяют признаки компьютерной инфекции и способы обнаружения вирусов. | |
| Выбирает и применяет средства для защиты компьютера от вредоносных программ. | |
| 4. Защита сетевых устройств и операционных систем. | | | | | Настраивает безопасность граничных маршрутизаторов и обеспечивает безопасный административный доступ. | |
| Идентифицирует типичные угрозы безопасности операционных систем. | |
| Применяет соответствующие меры для уменьшения уязвимостей ОС. | |
| 5. Знают о средствах обнаружения атак и методах обработки инцидентов в области информационной безопасности. | | | | | Оценивает необычную активность в сети и использовать средства обнаружения атак для реагирования на инциденты. | |
| **Пререквизиты** | Инструмент для анализа Big Data, Проектирование интеллектуальных систем управления | | | | | | |
| **Постреквизиты** | Дипломная работа | | | | | | |
| **Учебные ресурсы** | **Основная литература:**  1. Компьютерная безопасность: анализ угроз и защита. Уильям Столлинг, Чарльз Хоффман,  2. Киберпреступность: оценка и реагирование. Джеймс Ф. Бреннер, Джудит М. Бреннер.  **Дополнительная литература:**  1. Компьютерные преступления и цифровые расследования. Иэна У. Хоулд.  2. Безопасность компьютерных сетей. Пер. с англ. Эндрю Таненбаум.  Интернет-ресурсы  1. http://www.ifac-control.org/  2.http://www.mathnet.ru/ | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Академическая политика дисциплины** | | Академическая политика дисциплины определяется [Академической политикой](https://univer.kaznu.kz/Content/instructions/%D0%90%D0%BA%D0%B0%D0%B4%D0%B5%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B0.pdf) и [Политикой академической честности КазНУ имени аль-Фараби.](https://univer.kaznu.kz/Content/instructions/%D0%9F%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B0%20%D0%B0%D0%BA%D0%B0%D0%B4%D0%B5%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9%20%D1%87%D0%B5%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D0%B8.pdf)  Документы доступны на главной странице ИС Univer.  **Интеграция науки и образования.** Научно-исследовательская работа студентов, магистрантов и докторантов – это углубление учебного процесса. Она организуется непосредственно на кафедрах, в лабораториях, научных и проектных подразделениях университета, в студенческих научно-технических объединениях. Самостоятельная работа обучающихся на всех уровнях образования направлена на развитие исследовательских навыков и компетенций на основе получения нового знания с применением современных научно-исследовательских и информационных технологий. Преподаватель исследовательского университета интегрирует результаты научной деятельности в тематику лекций и семинарских (практических) занятий, лабораторных занятий и в задания СРОП, СРО, которые отражаются в силлабусе и отвечают за актуальность тематик учебных занятий и заданий.  **Посещаемость.** Дедлайн каждого задания указан в календаре (графике) реализации содержания дисциплины. Несоблюдение дедлайнов приводит к потере баллов.  **Академическая честность.** Практические/лабораторные занятия, СРО развивают у обучающегося самостоятельность, критическое мышление, креативность. Недопустимы плагиат, подлог, использование шпаргалок, списывание на всех этапах выполнения заданий.  Соблюдение академической честности в период теоретического обучения и на экзаменах помимо основных политик регламентируют [«Правила проведения итогового контроля»](https://univer.kaznu.kz/Content/instructions/%D0%9F%D1%80%D0%B0%D0%B2%D0%B8%D0%BB%D0%B0%20%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F%20%D0%B8%D1%82%D0%BE%D0%B3%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE%20%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8F%20%D0%9B%D0%AD%D0%A1%202022-2023%20%D1%83%D1%87%D0%B3%D0%BE%D0%B4%20%D1%80%D1%83%D1%81%D1%8F%D0%B7%D1%8B%D0%BA%D0%B5.pdf), [«Инструкции для проведения итогового контроля осеннего/весеннего семестра текущего учебного года»](https://univer.kaznu.kz/Content/instructions/%D0%98%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D0%B8%D1%8F%20%D0%B4%D0%BB%D1%8F%20%D0%B8%D1%82%D0%BE%D0%B3%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE%20%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8F%20%D0%B2%D0%B5%D1%81%D0%B5%D0%BD%D0%BD%D0%B5%D0%B3%D0%BE%20%D1%81%D0%B5%D0%BC%D0%B5%D1%81%D1%82%D1%80%D0%B0%202022-2023.pdf), «Положение о проверке текстовых документов обучающихся на наличие заимствований».  Документы доступны на главной странице ИС Univer.  **Основные принципы инклюзивного образования.** Образовательная среда университета задумана как безопасное место, где всегда присутствуют поддержка и равное отношение со стороны преподавателя ко всем обучающимся и обучающихся друг к другу независимо от гендерной, расовой/ этнической принадлежности, религиозных убеждений, социально-экономического статуса, физического здоровья студента и др. Все люди нуждаются в поддержке и дружбе ровесников и сокурсников. Для всех студентов достижение прогресса скорее в том, что они могут делать, чем в том, что не могут. Разнообразие усиливает все стороны жизни.  Все обучающиеся, особенно с ограниченными возможностями, могут получать консультативную помощь по телефону/е-mail: [adia\_kz@bk.ru](mailto:adia_kz@bk.ru) либо посредством видеосвязи в MSTeams*.*  **Интеграция МООC (massiveopenonlinecourse).**В случае интеграции МООCв дисциплину, всем обучающимся необходимо зарегистрироваться на МООC. Сроки прохождения модулей МООCдолжны неукоснительно соблюдаться в соответствии с графиком изучения дисциплины.  **ВНИМАНИЕ!** Дедлайн каждого задания указан в календаре (графике) реализации содержания дисциплины, а также в МООC. Несоблюдение дедлайнов приводит к потере баллов. | | | | |
| **ИНФОРМАЦИЯ О ПРЕПОДАВАНИИ, ОБУЧЕНИИ И ОЦЕНИВАНИИ** | | | | | | |
| **Балльно-рейтинговая**  **буквенная система оценки учета учебных достижений** | | | | | **Методы оценивания** | |
| **Оценка** | **Цифровой**  **эквивалент**  **баллов** | | **Баллы,**  **% содержание** | **Оценка по традиционной системе** | **Критериальное оценивание** – процесс соотнесения реально достигнутых результатов обучения с ожидаемыми результатами обучения на основе четко выработанных критериев. Основано наформативном и суммативном оценивании.  **Формативное оценивание –** вид оценивания, который проводится входе повседневной учебной деятельности. Является текущим показателем успеваемости. Обеспечивает оперативную взаимосвязь между обучающимся и преподавателем. Позволяет определить возможности обучающегося, выявить трудности, помочь в достижении наилучших результатов, своевременно корректировать преподавателю образовательный процесс. Оценивается выполнение заданий, активность работы в аудитории во время лекций, семинаров, практических занятий (дискуссии, викторины, дебаты, круглые столы, лабораторные работы и т. д.). Оцениваются приобретенные знания и компетенции.  **Суммативное оценивание**–вид оценивания, который проводится по завершению изучения раздела в соответствии с программой дисциплины. Проводится 3-4 раза за семестр при выполнении СРО. Это оценивание освоения ожидаемых результатов обучения в соотнесенности с дескрипторами. Позволяет определять и фиксировать уровень освоения дисциплины за определенный период. Оцениваются результаты обучения. | |
| A | 4,0 | | 95-100 | Отлично |
| A- | 3,67 | | 90-94 |
| B+ | 3,33 | | 85-89 | Хорошо |
| B | 3,0 | | 80-84 | **Формативное и суммативное оценивание** | **Баллы % содержание** |
| B- | 2,67 | | 75-79 | Активность на лекциях | 5 |
| C+ | 2,33 | | 70-74 | Работа на практических занятиях | 20 |
| C | 2,0 | | 65-69 | Удовлетворительно | Самостоятельная работа | 25 |
| C- | 1,67 | | 60-64 | Проектная и творческая деятельность | 10 |
| D+ | 1,33 | | 55-59 | Неудовлетворительно | Итоговый контроль (экзамен) | 40 |
| D | 1,0 | | 50-54 | ИТОГО | 100 |
| **Календарь (график) реализации содержания дисциплины. Методы преподавания и обучения.** | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Неделя** | **Название темы** | **Кол-во часов** | **Макс.**  **балл** |
| **МОДУЛЬ 1.** Основы Информационной Безопасности | | | |
| 1 | **Л1.** Введение в информационную безопасность | **2** | **2** |
| **ЛЗ 1.** Основы конфигурирования в командной строке IOS | 1 | 10 |
| 2 | **Л2**. Классификация компьютерных преступлений | 2 | 2 |
| **ЛЗ 2.**Основымоделированиякомпьютернойсети  в Cisco Packet Tracer | 1 | 10 |
| 3 | **Л3.** Пользователи и злоумышленники в Интернете | **2** | **2** |
| **ЛЗ 3.** Эмулятор оборудования Cisco GNS3 | 1 | 10 |
| **СРО 1.** Напишите реферат на тему "Информационная безопасность в современном мире", включая основные принципы и вызовы |  | 8 |
| 4 | **Л4.** Защита от компьютерных вирусов и заражение компьютера | **2** | **2** |
| **ЛЗ 4.** Операционная система Cisco IOS | 1 | 10 |
| **СРОП 1.** Консультация по выполнению **СРО 1.** |  |  |
| 5 | **Л5.** Средства противодействия угрозам безопасности | **2** | **2** |
| **ЛЗ 5.** Конфигурирование коммутаторов | 1 | 10 |
| **МОДУЛЬ 2.** Управление Безопасностью ИТ-Среды и Контроль Целостности | | | |
| 6 | **Л6.** Архитектура управления безопасностью ИТ-среды | **2** | **2** |
| **ЛЗ 6.** Конфигурирование маршрутизаторов | 1 | **10** |
| **СРОП 2.** Консультация по выполнению **СРО 1.** |  |  |
| 7 | **Л7.** Виды средств контроля целостности данных, цифровые подписи и сертификаты | **2** | **2** |
| **ЛЗ 7.** Конфигурирование протоколов управления оборудованием | **1** | **10** |
| **СРО 2.** Задание: Проанализируйте известные случаи компьютерных преступлений и выберите один, чтобы подготовить презентацию об этом инциденте. |  | **8** |
| **Рубежный контроль 1** | | | **100** |
| 8 | **Л8.** Обеспечение целостности баз данных | **2** | **2** |
| **ЛЗ 8.** Списки управления доступом | **1** | **10** |
| **СРОП 3.** Консультация по выполнению **СРО 2.** |  |  |
| 9 | **Л9.** Аутентификация, авторизация и учет | **2** | **2** |
| **ЛЗ 9.** Настройка Zone-Based Policy Firewall | **1** | **10** |
| **СРО 3.** Улучшение плана перевозок. Цикл пересчёта |  | **7** |
| 10 | **Л10.** Угрозы безопасности операционных систем | **2** | **2** |
| **ЛЗ 10.** Межсетевыеэкраны CiscoPIX | **1** | **10** |
| **СРОП 4.** Консультация по выполнению **СРО 3.** |  |  |
| **МОДУЛЬ 3.** Защита Операционных Систем и Обнаружение Атак | | | |
| 11 | **Л11.** Обеспечение безопасности сетевых устройств | **2** | **2** |
| **ЛЗ 11.** Организация защищенного канала на основе IPSec | **1** | **10** |
| 12 | **Л12.** Системы обнаружения атак и технологии обнаружения атак | **2** | **2** |
| **ЛЗ 12.** Настройка комплекса Cisco IDS Sensor | **1** | **10** |
| **СРОП 5.** Консультация по выполнению **СРО 3.** |  |  |
| 13 | **Л13.** Линейное программирование и симплекс-методы | **2** | **2** |
| **ЛЗ 13.** Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco IDS Sensor | **1** | **10** |
| **СРОП 6.** Консультация по выполнению **СРО 4.** |  |  |
| 14 | **Л14.** Проактивная безопасность и планирование инцидентов | **2** | **2** |
| **ЛЗ 14.** Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco MARS | **1** | **10** |
| **15** | **Л15.** Управление инцидентами и реагирование на угрозы | **2** | **2** |
| **ЛЗ 15.** Обнаружение компьютерных атак на узлы сети с использованием СОА Cisco Security Agent и Cisco MARS | **1** | **10** |
| **СРО 4.** Подготовьте учебные материалы или презентацию для обучения сотрудников организации основам информационной безопасности. Включите в них актуальные угрозы и методы предотвращения. |  | **7** |
| **Рубежный контроль2** | | | **100** |
| **Итоговый контроль (экзамен)** | | | **100** |
| **ИТОГО за дисциплину** | | | **100** |

**Декан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Лектор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**