**СИЛЛАБУС**

**Осенний семестр 2023-2024 учебного года**

**Образовательная программа** «7M06302 – Аудит информационной безопасности»

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID и наименование дисциплины** | | | **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)** |
| 98856 Анализ безопасности ОС | | | 4 | | | 1,7 | 0 | 3,3 | 5 | 7 |
| **АКАДЕМИЧЕСКАЯ ИНФОРМАЦИЯ О ДИСЦИПЛИНЕ** | | | | | | | | | | |
| **Формат обучения** | | | **Цикл,**  **компонент** | | **Типы лекций** | | **Типы практических занятий** | | **Форма и платформа**  **итогового контроля** | |
| *офлайн* | | | ПД. Вузовский компонент | | Информационная, аналитическая лекция | | Выполнение заданий по администрированию и настройке ОС | | Проект, Moodle | |
| **Лектор - (ы)** | | | Карюкин Владислав Игоревич | | | | | |
| **e-mail:** | | | vladislav.karyukin@gmail.com | | | | | |
| **Телефон:** | | | +77019405992 | | | | | |
| **Ассистент- (ы)** | | | – | | | | | |
| **e-mail:** | | | – | | | | | |
| **Телефон:** | | | – | | | | | |
| **АКАДЕМИЧЕСКАЯ ПРЕЗЕНТАЦИЯ ДИСЦИПЛИНЫ** | | | | | | | | | | |
| **Цель дисциплины** | | | **Ожидаемые результаты обучения (РО)\*** | | | | | | **Индикаторы достижения РО (ИД)** | |
| Цель дисциплины - применить требования информационной безопасности и навыков в использовании методов обеспечения защиты информации в ОС. Будут изучены: Методы и средства тестирования и защиты программ операционных систем. Принципы грамотного администрирования операционных систем. Методы анализа источников и угроз безопасности в операционных системах; средства и методы, направленные на устранение угроз безопасности в ОС. | | | 1. Изучать теорию операционных систем и их администрирования | | | | | | * 1. Изучить базовые компоненты операционных систем | |
| 1.2 Знать методы управления операционными системами | |
| 2. Уметь устанавливать виртуальные операционные системы | | | | | | 2.1 Создавать виртуальные машины | |
| 2.2 Устанавливать операционные системы на виртуальные машины | |
| 3. Уметь управлять процессами в операционных системах | | | | | | 3.1 Запускать диспетчер задач | |
| 3.2 Запускать и отключать определенные процессы в операционной системе | |
| 4. Управлять настройками файловой системы | | | | | | 4.1 Защищать файлы от несанкционированного доступа | |
| 4.2 Изменять тип файловой системы дисков операционной системы | |
| 5. Применять методы машинного обучения для обеспечения информационной безопасности | | | | | | 5.1 Исследовать применение машинного обучения в информационной безопасности | |
| 5.2 Разрабатывать системы, использующие модели машинного обучения | |
| **Пререквизиты** | | | Безопасность программных приложений | | | | | | | |
| **Постреквизиты** | | | Аудит информационной безопасности | | | | | | | |
| **Учебные ресурсы** | | | **Литература:** основная, дополнительная.  **Основная:**   * + - 1. Operating Systems: Internals and Design Principles by William Stallings, 2013       2. Operating System Concepts, 10th Edition by [Abraham Silberschatz](https://www.amazon.com/Abraham-Silberschatz/e/B000APPDZ2/ref=dp_byline_cont_ebooks_1), [Greg Gagne](https://www.amazon.com/s/ref=dp_byline_sr_ebooks_2?ie=UTF8&field-author=Greg+Gagne&text=Greg+Gagne&sort=relevancerank&search-alias=digital-text), [Peter B. Galvin](https://www.amazon.com/Peter-B-Galvin/e/B00DDCKS5O/ref=dp_byline_cont_ebooks_3), 2018       3. Guide to Operating Systems 5th Edition by [Greg Tomsho](https://www.amazon.com/Greg-Tomsho/e/B001JRVU52/ref=dp_byline_cont_book_1), 2016       4. Understanding Operating Systems by [Ann McHoes](https://www.amazon.com/s/ref=dp_byline_sr_ebooks_1?ie=UTF8&field-author=Ann+McHoes&text=Ann+McHoes&sort=relevancerank&search-alias=digital-text), [Ida M. Flynn](https://www.amazon.com/s/ref=dp_byline_sr_ebooks_2?ie=UTF8&field-author=Ida+M.+Flynn&text=Ida+M.+Flynn&sort=relevancerank&search-alias=digital-text), 2017       5. Windows 10 All-in-One For Dummies by [Woody Leonhard](https://www.amazon.com/Woody-Leonhard/e/B000APEHHW/ref=dp_byline_cont_book_1), 2015   **Дополнительная**: Windows Internals, Part 2 (Developer Reference) 7th Edition by [Andrea Allievi](https://www.amazon.com/s/ref=dp_byline_sr_book_1?ie=UTF8&field-author=Andrea+Allievi&text=Andrea+Allievi&sort=relevancerank&search-alias=books), [Mark Russinovich](https://www.amazon.com/s/ref=dp_byline_sr_book_2?ie=UTF8&field-author=Mark+Russinovich&text=Mark+Russinovich&sort=relevancerank&search-alias=books), [Alex Ionescu](https://www.amazon.com/s/ref=dp_byline_sr_book_3?ie=UTF8&field-author=Alex+Ionescu&text=Alex+Ionescu&sort=relevancerank&search-alias=books), [David Solomon](https://www.amazon.com/s/ref=dp_byline_sr_book_4?ie=UTF8&field-author=David+Solomon&text=David+Solomon&sort=relevancerank&search-alias=books), 2021Architectural and Operating System Support for Virtual Memory by [Abhishek Bhattacharjee](https://link.springer.com/book/10.1007/978-3-031-01757-5#author-0-0), [Daniel Lustig](https://link.springer.com/book/10.1007/978-3-031-01757-5#author-0-1), 2018 **Исследовательская инфраструктура**   1. Бизнес инкубатор № 12 2. Лабораторный кабинет 517 3. Лабораторный кабинет 323   **Профессиональные научные базы данных**  **Интернет-ресурсы**   * + - 1. <https://www.coursera.org/specializations/codio-introduction-operating-systems>       2. <https://www.coursera.org/learn/introduction-to-computers-and-operating-systems-and-security>       3. <https://www.coursera.org/learn/operating-system-foundations>   **Программное обеспечение**  **1.** Windows 10, Windows 11  **2.** Ubuntu  **3.** Kali Linux | | | | | | | |
| **Академическая политика дисциплины** | | | Академическая политика дисциплины определяется [Академической политикой](https://univer.kaznu.kz/Content/instructions/Академическая%20политика.pdf) и [Политикой академической честности КазНУ имени аль-Фараби.](https://univer.kaznu.kz/Content/instructions/Политика%20академической%20честности.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 изаданий.  **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/Правила%20проведения%20итогового%20контроля%20ЛЭС%202022-2023%20учгод%20русязыке.pdf), [«Инструкции для проведения итогового контроля осеннего/весеннего семестра текущего учебного года»](https://univer.kaznu.kz/Content/instructions/Инструкция%20для%20итогового%20контроля%20весеннего%20семестра%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 [*vladislav.karyukin@gmail.com*](mailto:vladislav.karyukin@gmail.com) */ +77019405992* либо посредством видеосвязи в MS Teams*.* | | | | | | | |
| **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 на формативном и суммативном оценивании.  **Формативное оценивание –** вид оценивания, который проводится в ходе 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 Введение в нейронные сети** | | | |
| 1 | **Л 1.** Анализ методов защиты операционных систем | 1 | 0 |
| **ЛЗ 1.** Описание различных методов защиты операционных систем | 2 | 5 |
| 2 | **Л 2.** Анализ существующих угроз в операционных системах | 1 | 0 |
| **ЛЗ 2.** Описание различных видов угроз операционных систем | 2 | 5 |
| **СРОП 1.** Консультации по выполнению СРО 1 |  |  |
| 3 | **Л 3.** Изучение основ администрирование Windows 10/11 | 1 | 0 |
| **ЛЗ 3.** Настройка Windows 10/11 | 2 | 10 |
| **СРО 1.** Настройка учетных записей безопасности доступа к Windows 10/11 |  | 20 |
| 4 | **Л 4.** Настройка служб Windows 10/11 | 1 | 0 |
| **ЛЗ 4.** Управление системными службами и процессами Windows | 2 | 10 |
| **СРОП 2.** Прием СРО 1 |  |  |
| 5 | **Л 5.** Анализ NTFS, FAT файловых систем Windows 10/11 | 1 | 0 |
| **ЛЗ 5.** Управление ресурсами в ОС Windows | 2 | 10 |
| **СРОП 3.** Консультация по выполнению СРО 2 |  |  |
| **МОДУЛЬ 2 Различные виды нейронных сетей** | | | |
| 6 | **Л 6.** Управление и настройка резервных копий ОС Windows 10/11 | 1 | 0 |
| **ЛЗ 6.** Восстановление работоспособности ОС Windows 10/11 | 2 | 10 |
| **СРО 2.** Настройка брандмауэров в ОС Windows 10/11 |  | 20 |
| 7 | **Л 7.** Управление и настройка списков контроля доступа в Windows 10/11 | 1 | 0 |
| **ЛЗ 7.** Создание списка контроля доступа в Windows 10/11 | 2 | 10 |
| **СРОП 4**. Прием СРО 2 |  |  |
| **Рубежный контроль 1** | | | **100** |
| 8 | **Л 8.** Изучение основ безопасности в ОС Linux | 1 | 0 |
| **ЛЗ 8.** Настройка параметров ОС Linux в командной строке | 2 | 10 |
| **СРОП 5.** Консультации по выполнению СРО 3 |  |  |
| 9 | **Л 9.** Управление сетевыми устройствами в Windows 10/11, Linux | 1 | 0 |
| **ЛЗ 9.** Настройка сетевых адресов в Windows 10/11, Linux | 2 | 10 |
| **СРО 3.** Настройка расширенных параметров доступа к системе ОС Linux |  | 10 |
| 10 | **Л 10.** Управление параметрами доступа в ОС Linux | 1 | 0 |
| **ЛЗ 10.** Создание учетных записей в ОС Linux | 2 | 10 |
| **СРОП 6.** Прием СРО 3 |  |  |
| **МОДУЛЬ 3 Большие модели нейронных сетей** | | | |
| 11 | **Л 11.** Анализ безопасности облачных служб | 1 | 0 |
| **ЛЗ 11.** Управление и настройка безопасности облачных служб | 2 | 10 |
| **СРПО 7.** Консультация по выполнению СРО 4 |  |  |
| 12 | **Л12.** Анализ безопасности сетевых соединений | 1 | 0 |
| **ЛЗ 12.** Конфигурация безопасности сетевых устройств | 2 | 10 |
| **СРО 4.** Создание облачной инфраструктуры |  | 10 |
| 13 | **Л 13.** Анализ защищенности удаленного доступа | 1 | 0 |
| **ЛЗ 13.** Создание и настройка VPN | 2 | 10 |
| 14 | **Л 14.** Использование моделей машинного обучения для защиты приложений ОС | 1 | 0 |
| **ЛЗ 14.** Разработка моделей машинного обучения для безопасности ОС | 2 | 10 |
| 15 | **Л 15.** Анализ веб-приложений, использующих модели машинного обучения | 1 | 0 |
| **ЛЗ 15.** Разработка веб-приложения, использующего методы машинного обучения | 2 | 10 |
| **Рубежный контроль 2** | | | **100** |
| **Итоговый контроль (экзамен)** | | | **100** |
| **ИТОГО за дисциплину** | | | **100** |

**Декан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Урмашев Б.А.**

**Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Мусиралиева Ш.Ж.**

**Лектор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Карюкин В.И.**

**РУБРИКАТОР СУММАТИВНОГО ОЦЕНИВАНИЯ**

**КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ**

**СРО 1. Настройка учетных записей безопасности доступа к Windows 10/11 (20% от 100% РК1)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Критерий** | **«Отлично»**  16-20% | **«Хорошо»**  11-15% | **«Удовлетворительно»**  6-10% | **«Неудовлетворительно»**  0-5% |
| Знание и понимание основных методов настройки учетных записей безопасности доступа к Windows 10/11 | Понимание степени соответствия, актуальности и достоверности найденных данных. Знание и понимание всех основных настроек безопасности учетных записей доступа к Windows 10/11 | Понимание степени соответствия, актуальности и достоверности найденных данных. Знание больше части настроек безопасности учетных записей доступа к Windows 10/11 | Ограниченное понимание степени соответствия, актуальности и достоверности настроек безопасности учетных записей доступа к Windows 10/11 | Поверхностное понимание/ отсутствие понимания степени соответствия, актуальности и достоверности найденных данных.   Отсутствие знания настроек безопасности учетных записей доступа к Windows 10/11 |
| Навыки настройки учетных записей безопасности доступа к Windows 10/11 | Четкое и ясное представление настройки учетных записей безопасности доступа к Windows 10/11 | Имеются логические ошибки настройки учетных записей безопасности доступа к Windows 10/11 | Большое количество логических ошибок настройки учетных записей безопасности доступа к Windows 10/11 | Отсутствие настройки учетных записей безопасности доступа к Windows 10/11 |
| Написание отчета | Письмо демонстрирует ясность, лаконичность и правильность. | Письмо демонстрирует ясность, лаконичность и корректность. В основном отсутствуют ошибки. | В письме есть некоторые ключевые ошибки, и ясность нуждается в улучшении. | Написанное неясно, трудно следовать за содержанием. Много ошибок в тексте |

**СРО2. Настройка брандмауэров в ОС Windows 10/11** **(20% от 100% РК1)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Критерий** | **«Отлично»**  16-20% | **«Хорошо»**  11-15% | **«Удовлетворительно»**  6-10% | **«Неудовлетворительно»**  0-5% |
| Работа с настройкой брандмауэров в ОС Windows 10/11 | Понимание степени соответствия, актуальности и достоверности работы с настройкой брандмауэров в ОС Windows 10/11 | Понимание степени соответствия, актуальности и достоверности настройки брандмауэров в ОС Windows 10/11 | Ограниченное понимание степени соответствия, актуальности и достоверности настройки брандмауэров в ОС Windows 10/11 | Поверхностное понимание/ отсутствие понимания степени соответствия, актуальности и достоверности настройки брандмауэров в ОС Windows 10/11 |
| Навыки настройки брандмауэров в ОС Windows 10/11 | Четкое и ясное представление настройки брандмауэров в ОС Windows 10/11 | Имеются небольшие логические ошибки настройки брандмауэров в ОС Windows 10/11 | Большое количество логических и синтаксических ошибок настройки брандмауэров в ОС Windows 10/11 | Отсутствие настройки брандмауэров в ОС Windows 10/11 |
| Написание отчета | Письмо демонстрирует ясность, лаконичность и правильность. | Письмо демонстрирует ясность, лаконичность и корректность. В основном отсутствуют ошибки. | В письме есть некоторые ключевые ошибки, и ясность нуждается в улучшении. | Написанное неясно, трудно следовать за содержанием. Много ошибок в тексте |

**СРО3. Настройка расширенных параметров доступа к системе ОС Linux (10% от 100% РК2)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Критерий** | **«Отлично»**  9-10% | **«Хорошо»**  6-8% | **«Удовлетворительно»**  3-5% | **«Неудовлетворительно»**  0-2% |
| Работа с настройкой расширенных параметров доступа к системе ОС Linux | Понимание степени соответствия, актуальности и достоверности настройки расширенных параметров доступа к системе ОС Linux | Понимание степени соответствия, актуальности и достоверности настройки расширенных параметров доступа к системе ОС Linux | Ограниченное понимание степени соответствия, актуальности и достоверности настройки расширенных параметров доступа к системе ОС Linux | Поверхностное понимание/ отсутствие понимания степени соответствия, актуальности и достоверности настройки расширенных параметров доступа к системе ОС Linux |
| Навыки настройки расширенных параметров доступа к системе ОС Linux | Четкое и ясное представление настройки расширенных параметров доступа к системе ОС Linux | Имеются небольшие логические ошибки настройки расширенных параметров доступа к системе ОС Linux | Большое количество логических и синтаксических ошибок настройки расширенных параметров доступа к системе ОС Linux | Отсутствие настройки расширенных параметров доступа к системе ОС Linux |
| Написание отчета | Письмо демонстрирует ясность, лаконичность и правильность. | Письмо демонстрирует ясность, лаконичность и корректность. В основном отсутствуют ошибки. | В письме есть некоторые ключевые ошибки, и ясность нуждается в улучшении. | Написанное неясно, трудно следовать за содержанием. Много ошибок в тексте |

**СРО4. Создание облачной инфраструктуры (10% от 100% РК2)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Критерий** | **«Отлично»**  9-10% | **«Хорошо»**  6-8% | **«Удовлетворительно»**  3-5% | **«Неудовлетворительно»**  0-2% |
| Создание облачной инфраструктуры | Понимание степени соответствия, актуальности и достоверности создания облачной инфраструктуры | Понимание степени соответствия, актуальности и достоверности создания облачной инфраструктуры | Ограниченное понимание степени соответствия, актуальности и достоверности создания облачной инфраструктуры | Поверхностное понимание/ отсутствие понимания степени соответствия, актуальности и достоверности создания облачной инфраструктуры |
| Навыки создания облачной инфраструктуры | Четкое и ясное представление облачной инфраструктуры | Имеются небольшие логические ошибки создания облачной инфраструктуры | Большое количество логических и синтаксических ошибок в создании облачной инфраструктуры | Отсутствие облачной инфраструктуры |
| Написание отчета | Письмо демонстрирует ясность, лаконичность и правильность. | Письмо демонстрирует ясность, лаконичность и корректность. В основном отсутствуют ошибки. | В письме есть некоторые ключевые ошибки, и ясность нуждается в улучшении. | Написанное неясно, трудно следовать за содержанием. Много ошибок в тексте |