**Силлабус**

**Осенний семестр 2020-2021 у.г.**

**По образовательной программе «6M070300 – Информационные системы»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Код дисциплины** |  **Название дисциплины** | **СРМ** | **Кол-во часов**  | **Кол-во кредитов** | **СРМП** |
| **Лекц.** | **Практ.** | **Лабор.** |
| UBIS 6306 | Управление безопасностью информационных систем | 85 | 15 |  | 30 | 5 | 5 |
| **Академическая информация о курсе** |
| Вид обучения | Тип/характер курса  | Тип лекции | Типы практических занятий  | Кол-во СРМ | Тип итогового контроля |
| Оffлайн /объединенная | теоретический | Аналитическая  | Лабораторные работы | три | Письменный экзамен |
| **Лектор** | Азанов Николай Прокопьевич, к. ф.-м. н., доцент. | **Оф./с.** | По расписанию |
| **e-mail** | E-mail: Nikolai.Azanov@kaznu.kz |
| **Телефон**  | Телефон: 87052092966 |  |  |

|  |
| --- |
| **Академическая презентация курса** |

|  |  |  |
| --- | --- | --- |
| **Цель дисциплины** | **Ожидаемые результаты обучения (РО)** | **Индикаторы достижения РО** (на каждый РО не менее 2-х индикаторов) |
| Помощь в овладении теоретическими знаниями и формировании практических умений и навыков в области обеспечения надежности и безопасности программного обеспечения (ПО) современных технических систем, и прежде всего в освоении комплекса мер, методов и способов защиты ПО от непреднамеренных и преднамеренных программных воздействий. | **РО** 1 (когнитивный) Знать основы деятельности государства в условиях информационного противоборства; основные положения теории надежности и безопасности ИС; нормативные правовые документы в области функциональной надежности, функциональной и информационной безопасности; математические модели надежности и безопасности ПО; модели и методы защиты операционных систем; основные проектные решения, средства и методы защиты ПО от непреднамеренных дефектов и вредоносных программ | **1.1** - осуществлять критический анализ проблемных ситуаций на основе системного подхода**1.2** - вырабатывать программу действий для проблемных ситуаций на основе системного подхода **1.3** - управлять проектом защиты ПО на всех этапах его жизненного цикла |
| **РО 2** (функциональный) Применять существующие методы защиты информации от несанкционированного доступа без снижения их стойкости вследствие принятия неправильных эксплуатационных решений  | **2.1** –решать типовые задачи с помощью методов надежности технических систем и защиты информации от несанкционированного доступа;**2.2** –прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты  |
| **РО 3** (функциональный) Применять современные методы и методики защиты ПО от непреднамеренных дефектов и вредоносных программ, от несанкционированного исследования, копирования, распространения и использования  | **3.1** –проводить обоснование состава, характеристик и функциональных возможностей систем, средств и технологий обеспечения информационной безопасности объектов защиты на основе казахстанских и международных стандартов;**3.2** –разрабатывать и проводить испытания систем, средств и технологий обеспечения информационной безопасности с применением соответствующих физических и математических методов, технических и программных средств;  |

|  |  |  |
| --- | --- | --- |
|  |  | **3.3** –организовать работу по созданию, модернизации и вводу в эксплуатацию систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами КНБ и Правительства Республики Казахстан  |
| **РО 4** (системный) Владеть методами разработки и использования защищенных программных средств  | **4.1** – проводить анализ процесса функционирования объекта защиты совместно с применяемыми информационными технологиями и техническими средствами с целью определения возможных источников информационных угроз, их вероятных целей и тактики воздействия на объект защиты;**4.2** – формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта и его информационных составляющих, с целью повышения их устойчивости к деструктивным воздействиям.  |
| **РО 5** (системный) Владеть навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах. | **5.1** – разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации **5.2** – провести выбор необходимых технологий и технических средств по обеспечению информационной безопасности объекта информатизации, организовать их внедрение и последующее сопровожде- ние**5.3** – организовать и сопровождать аттестацию объектов информатизации в соответствии с нормативными документами. |
| Пререквизиты и постреквизиты | **Пререквизиты:** нет**Постреквизиты:** нет |
| Литература и ресурсы | **Литература**: **Основная:**1. Замятина, О. М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей: учебное пособие для магистратуры / О. М. Замятина. – М.: Издательство Юрайт, 2016. — 159 с. — (Университеты России). — ISBN 978-5-9916-6531-5.2. Кенин А.М. Практическое руководство системного администратора. 2-е издание - СПб: БХВ-Петербург, 2013. –532с.3. Скабцов Н. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с. – (Серия «Библиотека программиста»). – ISBN 978-54461066224. Аверченков В.И. Аудит информационной безопасности: учеб. пособие для вузов / В.И. Аверченков. – 3-е изд., стереотип. – М.: ФЛИНТА, 2016. – 269 с – ISBN 978-5940743743**Дополнительная:**  указана в методических указаниях по выполнению СРМ **Список необходимых средств и материалов обучения:*** Текстовые и графические редакторы (различных масштабов и тематики)
* Компьютерные программы тестирования ПО

**Ресурсы:** **- Програмнное обеспчение и Интернет- ресурсы:**Microsoft Office, Power Point, Adobe Reader, Paint.**- базы данных, нформационно-справочные и поисковые системы:** специализированные веб-сайты и базы данных в интернет указаны в методических указаниях по выполнению СРМ**Онлайн достижимость:** дополнительные учебные материалы, задания для СРМ и лабораторных работ можно найти на своих страницах (УМКД) на сайте univer.kaznu.kz.  |

|  |  |
| --- | --- |
| Академическая политика курса в контексте университетских морально-этических ценностей | **Правила академического поведения:** 1. К каждому аудиторному занятию (лекции, лабораторной работе) вы должны подготовиться заранее, согласно графику, приведенному ниже. Подготовка задания должна быть завершена до аудиторного занятия, на котором обсуждается тема.
2. **Академические ценности:**
3. Лабораторные занятия, СРМ должны носить самостоятельный, творческий характер
4. Недопустимы плагиат, подлоги, использование шпаргалок, списывание на всех этапах контроля знаний

Обучающиеся с ограниченными возможностями могут получать консультационную помощь по Э- адресу \*\*\*\*\*\*\* |
| Политика оценивания и аттестации | **Критериальное оценивание:** оценивание результатов обучения в соотнесенности с дескрипторами (проверка сформированности компетенций на рубежном контроле и экзаменах).**Суммативное оценивание:** оценивание активности работы в аудитории; оценивание выполненного задания. |

**Календарь (график) реализации содержания учебного курса**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Неделя | Название темы | Результаты обучения (РО) | Индикаторы достижения РО | Кол-во часов | Макс балл | Форма оценки знаний |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **I** | **Модуль - Введение в надежность и безопасность информационных систем.** |
| 1 | **Лекция (**аналитическая**):**Общий обзор курса. Определение информационной безопасности. | РО 1  | 1.1 | 1 | 2 |  |
| 1 | **Лабораторное занятие:**Категории атак Методы хакеров **Тип задания:** Составление отчета | РО 1 | 1.1  | 2 | 10 | Отчет |
| 1 | **СРМ- 1.** Введение в надежность и безопасность информационных систем Задание 1**Тип задания:** Составление отчета | РО 1 | 1.1; 1.2; 1.3 | 6 | 8 | Отчет |
| 2 | **Лекция (**аналитическая**):**Политика. Управление риском. | РО 1  | 1.1 | 1 | 2 | Беседа- опрос |
| 2 | **Лабораторное занятие:**Юридические вопросы информационной безопасности**Тип задания:** Составление отчета | РО 1 | 1.1  | 2 | 10 | Отчет |
| 2 | **СРМ- 1.** Введение в надежность и безопасность информационных систем Задание 2.**Тип задания:** Составление отчета | РО 1 | 1.1; 1.2; 1.3 | 6 | 8 | Отчет |
| 3 | **Лекция** (аналитическая)Рекомендации по обеспечению сетевой безопасности. | РО 1 | 1.2; 1.3 | 1 | 2 | Беседа- опрос |
| 3 | **Лабораторное занятие:**Межсетевые экраны**Тип задания:** Составление отчета | РО 1 | 1.2; 1.3 | 4 | 10 | Отчет |
| 3 | **СРМ- 1.** Введение в надежность и безопасность информационных систем Задание 3.**Тип задания:** Составление отчета | РО 1 | 1.1; 1.2; 1.3 | 6 | 8 | Отчет |
| 4 | **Лекция** (аналитическая)Виртуальные частные сети | РО 1 | 1.2; 1.3 | 1 | 2 | Беседа- опрос |
| 4 | **Лабораторное занятие:**Шифрование**Тип задания:** Составление отчета | РО 1 | 1.2; 1.3 | 2 | 10 | Отчет |
| 4 | **СРМП 1 -** Проведение взаимного обсуждения и консультации по **СРМ 1** | РО 1 | 1.1; 1.2; 1.3 | 1 | 0 | Беседа |
| 4 | **СРМ- 1.** Введение в надежность и безопасность информационных систем Задание 4. **Тип задания:** Составление отчета | РО 1 | 1.1; 1.2; 1.3 | 5 | 8 | Отчет  |
| 5 | **Лекция** (аналитическая)Обнаружение вторжений | РО 1 | 1.2; 1.3 | 1 | 2 | Беседа- опрос |
| 5 | **Лабораторное занятие:**Безопасность UNIX**Тип задания:** Составление отчета | РО 1; РО 2 | 1.3; 2.1; 2.2 | 2 | 10 | Отчет  |
| 5 | **СРМ- 1.** Введение в надежность и безопасность программного обеспечения Задание 5. Угрозы надежности и безопасности программного обеспечения**Тип задания:** Составление отчета | РО 1 | 1.1; 1.2; 1.3 | 5 | 8 | Отчет  |
| 5 | **СРМП 2 -** Прием и оценка задания по **СРМ 1** | РО 1; РО 2 | 1.2; 1.3; 2.1; 2.2 | 1 | 0 | Собеседова-ние и защита |
| 5 | **РК 1 накопительный** |  |  |  | 100 |  |

|  |  |
| --- | --- |
| **II** | **Модуль - Предпосылки и основные направления развития менеджмента в сфере информационной безопасности** |
| 6 | **Лекция** (аналитическая)Вопросы безопасности Windows / Windows Server | РО 2 | 2.1 | 1 | 2 | Беседа- опрос |
| 6 | **Лабораторное занятие:**Электронная коммерция: требования к безопасности**Тип задания:** Составление отчета | РО 2 | 2.1 | 2 | 10 | Отчет |
| 6 | **СРМ- 2.** Предпосылки и основные направления развития менеджмента в сфере информационной безопасности Задание 1.**Тип задания:** Составление отчета | РО 2; РО 4 | 2.1; 2.2; 4.1 | 6 | 8 | Отчет |
| 7 | **Лекция (**аналитическая**)**Безопасность беспроводных соединений | РО 2 | 2.2 | 1 | 2 | Беседа- опрос |
| 7 | **Лабораторное занятие:**Цели, задачи, предпосылки и направления организационной и управленческой работы в сфере информационной безопасности**Тип задания:** Составление отчета | РО 2; РО 3; РО 4 | 2.2; 3.1; 4.1 | 2 | 10 | Отчет |
| 7 | **СРМ- 2.** Предпосылки и основные направления развития менеджмента в сфере информационной безопасности Задание 2.**Тип задания:** Составление отчета | РО 2; РО 4 | 2.1; 2.2; 4.1 | 6 | 8 | Отчет |
| 8 | **Лекция** (аналитическая)Предпосылки и основные направления развития менеджмента в сфере информационной безопасности | РО 3 | 3.1; 3.2; 3.3 | 1 | 2 | Беседа- опрос |
| 8 | **Лабораторное занятие:**Управление информационной безопасностью на уровне крупных поставщиков информационных тем **Тип задания:** Составление отчета | РО 3 | 3.1; 3.2; 3.3 | 2 | 10 | Отчет |
| 8 | **СРМ- 2.** Предпосылки и основные направления развития менеджмента в сфере информационной безопасности Задание 3.**Тип задания:** Составление отчета | РО 2; РО 4 | 2.1; 2.2; 4.1 | 5 | 8 | Отчет |
| 8 | **СРМП 3** Проведение взаимного обсуждения и консультации по **СРМ 2** | РО 2; РО 4 | 2.1; 2.2; 4.1 | 1 | 0 | Беседа |
|  9 | **Лекция (**аналитическая**)**Деятельность международных организаций в сфере информационной безопасности | РО 3 | 3.1: 3.2: 3.3 | 1 | 2 | Беседа- опрос |
| 9 | **Лабораторное занятие:**Управление информационной безопасностью на государственном уровне: Общие принципы и практика государств СНГ **Тип задания:** Составление отчета | РО 3; РО 4; РО 5 | 3.2; 4.1; 4.2; 5.1 | 2 | 10 | Отчет |
| 9 | **СРМ- 2.** Предпосылки и основные направления развития менеджмента в сфере информационной безопасности Задание 4.**Тип задания:** Составление отчета | РО 2; РО 4 | 2.1; 2.2; 4.1 | 6 | 8 | Отчет |
| 10 | **Лекция** (аналитическая)Управление информационной безопасностью на государственном уровне: Общие принципы и казахстанская практика | РО 3 | 3.1; 3.3 | 1 | 2 | Беседа- опрос |
| 10 | **Лабораторное занятие:**Прием заданий. Собеседование**Тип задания:** Составление отчета | РО 3; РО 4 | 3.1; 3.3; 4.2 | 2 | 10 | Отчет |
| 10 | **СРМ- 2.** Предпосылки и основные направления развития менеджмента в сфере информационной безопасности Задание 5.**Тип задания:** Составление отчета | РО 2; РО 4 | 2.1; 2.2; 4.1 | 6 | 8 | Отчет |
| 10 | **Midterm накопительный** |  |  |  | 100 |  |
| **III** | **Модуль - Методы и технологии обеспечения безопасности информационных систем.** |
| 11 | **Лекция** (аналитическая):Организационное обеспечение информационной безопасности на государственном уровне: практика США | РО 4 | 4.1; 4.2 | 1 | 2 | Беседа- опрос |
| 11 | **Лабораторное занятие:**Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности**Тип задания:** Составление отчета | РО 4 | 4.1; 4.2 | 2 | 10 | Отчет |
| 11 | **СРМ- 3.** Методы и технологии обеспечения безопасности информационных систем Задание 1.**Тип задания:** Составление отчета | РО 2; РО 4 | 2.1; 2.2; 4.1 | 5 | 8 | Отчет |
| 11 | **СРМП 4 –** Проведение взаимного обсуждения и консультации по **СРМ 3** | РО 3; РО 4 | 3.1; 3.2; 3.3; 4.1; 4.2 | 1 | 0 | Беседа |
| 12  | **Лекция** (аналитическая):Содержание детализированной политики безопасности | РО 4 | 4.1; 4.2 | 1 | 2 | Беседа- опрос |
| 12 | **Лабораторное занятие:**Департамент информационной безопасности и работа с персоналом **Тип задания:** Составление отчета | РО 4; РО 5 | 4.1; 4.2; 5.1; 5.2 | 2 | 10 | Отчет |
| 12 | **СРМ- 3.** Методы и технологии обеспечения безопасности информационных систем Задание 2.**Тип задания:** Составление отчета | РО 2; РО 4 | 2.1; 2.2; 4.1 | 6 | 8 | Отчет |
| 13 | **Лекция** (аналитическая):Организация реагирования на чрезвычайные ситуации (инциденты) | РО 5 | 5.1; 5.2 | 1 | 2 | Беседа- опрос |
| 13 | **Лабораторное занятие:**Аудит состояния информационной безопасности на предприятии **Тип задания:** Составление отчета | РО 5 | 5.1; 5.2 | 2 | 10 | Отчет |
| 13 | **СРМ- 3.** Методы и технологии обеспечения безопасности информационных систем Задание 3.**Тип задания:** Составление отчета | РО 2; РО 4 | 2.1; 2.2; 4.1 | 5 | 8 | Отчет |
| 13 | **СРМП 5 -** Проведение взаимного обсуждения и консультации по **СРМ 3** | РО 3; РО 4 | 3.1; 3.2; 3.3; 4.1; 4.2 | 1 | 0 | Беседа |
| 14 | **Лекция** (аналитическая):Программные средства, поддерживающие управление информационной безопасностью на предприятии | РО 5 | 5.1; 5.2; 5.3 | 1 | 2 | Беседа- опрос |
| 14  | **Лабораторное занятие:**Предоставление услуг в сфере информационной безопасности**Тип задания:** Составление отчета | РО 5 | 5.1; 5.2; 5.3 | 2 | 10 | Отчет  |
| 14 | **СРМ- 3.** Методы и технологии обеспечения безопасности информационных систем Задание 4.**Тип задания:** Составление отчета | РО 2; РО 4 | 2.1; 2.2; 4.1 | 5 | 8 | Отчет |
| 15 | **Лекция** (аналитическая):Экономика информационной безопасности. | РО 5 | 5.1; 5.2; 5.3 | 1 | 2 | Беседа- опрос |
| 15  | **Лабораторное занятие:**Прием заданий. Собеседование.**Тип задания:** Составление отчета | РО 5 | 5.1; 5.2; 5.3 | 2 | 10 | Отчет |
| 15 | **СРМ- 3.** Методы и технологии обеспечения безопасности информационных систем Задание 5.**Тип задания:** Составление отчета | РО 2; РО 4 | 2.1; 2.2; 4.1 | 6 | 8 | Отчет |
| 15 | **РК 2 накопительный** |  |  |  | 100 |  |

Декан ф-та, профессор Б.А. Урмашев

Председатель методбюро Ф.Р. Гусманова

Заведующий кафедрой Ш.Ж. Мусиралиева

Лектор, доцент Н.П. Азанов