НАО «Евразийский национальный университет им. Л. Н. Гумилева»
Факультет «Информационных технологий»
«Кафедра Технологии искусственного интеллекта»

Рабочая (модульная) учебная программа (Syllabus)

COMS 32010 Организация вычислительных систем по дисциплине
OK 3213 Основы кибербезопасности
для обучающихся по образовательной программе
6B06112 Технологии искусственного интеллекта

Астана
2025

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года «Об электронном документе и электронной цифровой подписи» равнозначен документу на бумажном носителе

Документ подписали

№	ФИО	Должность
1	Ниязова Розамгуль Сериковна	ассоциированный профессор (доцент)
2	Разахова Бибигул Шамшановна	Заведующий кафедры
3	Давлетова Айнаш Халиуллиновна	ассоциированный профессор (доцент)
4	Оразалиев Бахытжан Асетилдаевич	Директор
5	Сеилов Шахмаран Журсинбекович	Декан факультета

Разработчик:
Ниязова Розамгуль Сериковна, ассоциированный профессор (доцент)

Рабочая учебная программа (Syllabus) по дисциплине OK 3213 Основы кибербезопасности
(код и наименование дисциплины)
Разработана на основании образовательной программы 6B06112 Технологии искусственного
(шифр и наименование образовательной программы)
интеллекта

Рассмотрено на заседании кафедры «Технологии искусственного интеллекта» протокол №11 от «02» 06 2025 г.

Одобрено на заседании учебно-методической комиссии факультета протокол №11 от «5» 06 2025г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Краткое описание дисциплины: Дисциплина направлена на формирование базовых знаний и навыков в области кибербезопасности, необходимых для защиты информационных систем, данных и интеллектуальных технологий в цифровой среде. Изучаются основные угрозы и уязвимости, методы обеспечения конфиденциальности, целостности и доступности информации, основы криптографии, сетевой безопасности, а также законодательные и организационные аспекты информационной безопасности. Особое внимание уделяется вопросам защиты данных в системах, основанных на искусственном интеллекте (ИИ), включая приватность данных, противодействие атакам на модели ИИ , этические аспекты и соответствие международным стандартам (ISO/IEC 27001, 27032 и др.).

Цель дисциплины	Результаты обучения (РО) по образовательной программе *	Ожидаемые результаты обучения (РО) по дисциплине
Дисциплина «Основы кибербезопасности» направлена на изучение принципов защиты информации и систем от кибератак, включая угрозы и уязвимости, методы и технологии защиты, управление информационной безопасностью, правовые аспекты, и действия при инцидентах безопасности. -	$РО_8$ - Осуществлять выбор технологии, средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности, обеспечивать защиту информации в сети с использованием программно-аппаратных средств	$ОПК_4$ - способность применять навыки по компьютерным технологиям и использованию математического аппарата для представления знаний. Знать: - Основные понятия кибербезопасности, типы угроз и уязвимостей. - Методы защиты информации и системы безопасности. - Правовые аспекты кибербезопасности и стандарты. Уметь: - Идентифицировать и анализировать киберугрозы. - Применять методы защиты данных и сетей. - Реагировать на инциденты и восстанавливать системы. Иметь навыки: - Настройка и управление системами безопасности. - Использование инструментов для обнаружения и предотвращения атак. - Проведение аудитов безопасности и оценка рисков.

**Согласно* 6В06112 Технологии искусственного интеллекта*, 2022 г.*

2. Пререквизиты

Для освоения данной дисциплины необходимы знания, умения и навыки, приобретённые при изучении следующих дисциплин: не предусмотрено

Постреквизиты

Знания, умения и навыки, полученные при изучении дисциплины необходимы для освоения следующих дисциплин: РР 4307 Производственная практика

(название дисциплин)

3. Выписка из учебного плана

Курс 3

Семестр 6

Количество кредитов ECTS 5

Виды занятий	Общее количество часов
Лекции	15
Практические занятия	30
Семинарские занятия	
Лабораторные занятия	
Самостоятельная работа обучающегося (СРО)	105
Итого	150

4. Тематический план дисциплины по модулям

(в академических часах)

№ модуля	Наименование модуля
1	Введение в кибербезопасность
2	Кибербезопасность, уязвимости и атаки

Лекционные занятия				
№ недели	**№ модуля**	**Наименование темы лекции**	**Количество часов**	**Виды и методы обучения**
1	1	Угрозы кибербезопасности, уязвимости и атаки. Обеспечение безопасности сетей	1	объяснение на конкретных примерах, обсуждение
2	1	Атаки, уязвимости TCP/ UDP, уязвимости IP адресов. IP-услуги. Противодействие распространенным сетевым атакам.	1	Интерактивная лекция. Объяснение с помощью рисунков и моделей
3	1	Беспроводная сетевая связь. Инфраструктура сетевой безопасности	1	Проблемная лекция. Анализ качественных характеристик, Примеры кейсов
4	1	Обзор Linux. Основы Linux.. Работа в оболочке Linux.. Файловая система Linux.. Работа на хосте Linux. Работа с графическим интерфейсом Linux.	1	Лекция-семинар. Анализ кейсов, Системный анализ
5	1	Защита системы и конечных точек. Предотвращение вторжений на уровне хоста. Принципы, методы и процессы кибербезопасности. Меры противодействия кибербезопасности	1	Аналитическая лекция. Системная оценка, Сравнительный анализ
6	1	Политика, правила и стандарты безопасности. Защита систем и сетей. Укрепление безопасности беспроводных и мобильных устройств	1	Лекция-семинар. Анализ кейсов, Системный анализ
7	1	Концепции контроля доступа. Использование и эксплуатация AAA. ACL. Стандартный синтаксис именованных списков контроля доступа IPv4	1	объяснение на конкретных примерах, обсуждение
8	2	Технологии межсетевых экранов. Зональные межсетевые экраны. Операция ZPF. Настройка ZPF.	1	Интерактивная лекция. Объяснение с помощью рисунков и моделей
9	2	Безопасность облака. Безопасность	1	Проблемная лекция. Анализ

		облачных приложений. Защита виртуальных машин		качественных характеристик, Примеры кейсов
10	2	Криптография. Технологии и протоколы.	1	Лекция-семинар. Анализ кейсов, Системный анализ
11	2	Данные сетевой безопасности. Оценка оповещений.	1	Аналитическая лекция. Системная оценка, Сравнительный анализ
12	2	Управление и соответствие требованиям. Тестирование сетевой безопасности. Методы и инструменты тестирования сетевой безопасности	1	Интерактивная лекция. Разбор стандартов менеджмента рисков информационной безопасности
13	2	Анализ угроз. Оценка уязвимости конечных точек.	1	Интерактивная лекция. Объяснение с помощью рисунков и моделей
14	2	Управление рисками и меры безопасности	1	Проблемная лекция. Анализ качественных характеристик, Примеры кейсов
15	2	Цифровая криминалистика, анализ инцидентов и реагирование на них	1	Лекция-семинар. Анализ кейсов, Системный анализ. Подведение итогов
		ИТОГО	**15**	

Практические (семинарские) занятия				
№ недели	**№ модуля**	**Наименование тем практических (семинарских) занятий**	**Количество часов**	**Виды и методы обучения**
1	1	Packet Tracer — исследование ландшафта угроз	2	Практическая работа, практический метод закрепления теоретических знаний
2	1	Packet Tracer — настройка базовой безопасности беспроводной сети	2	Интерактивные задания
3	1	Packet Tracer — устранение неполадок беспроводного соединения	2	Кейс-стади
4	1	Навигация по файловой системе Linux и настройкам прав доступа	2	Кейс-стади
5	1	Онлайн-инструменты для расследования вредоносных программ	2	Кейс-стади
6	1	Документирование проблем кибербезопасности предприятия	2	Проектная работа
7	1	Packet Tracer — реализация физической безопасности с помощью устройств Интернета вещей	2	Симуляция и игра
8	1	Packet Tracer — настройка аутентификации на основе сервера с помощью TACACS+ и RADIUS	2	Обратная связь и обзор
9	2	Packet Tracer — настройка расширенных списков ACL, сценарий 2	2	Ролевые игры
10	2	Packet Tracer — настройка ZPF	2	Анализ конкретных ситуаций
ю11	2	Packet Tracer — изучение реализации NetFlow Packet Tracer — ведение журнала из нескольких источников	2	Анализ конкретных ситуаций

12	2	Классифицирование оповещения	2	Гонки и хакатоны
13	2	Используйте Wireshark для сравнения трафика Telnet и SSH Анализ сетевого трафика с помощью программы Wireshark	2	Мастер-классы и гостевые лекции
14	2	Определить соответствующие данные об угрозах. Реализация мер безопасности	2	Мастер-классы и гостевые лекции
15	2	Packet Tracer — исследование аварийного восстановления Рекомендация мер по аварийному восстановлению	2	обзор по практическому занятию
		ИТОГО	**30**	

СРО				
№ недели	**№ модуля**	**Наименование темы СРО. Сроки сдачи СРО**	**Количество часов**	**Виды и методы обучения**
1	1	Понятие информационной безопасности. Основные составляющие.	**7**	Поиск и метод исследования
2	1	Распространение объектно-ориентированного подхода к информационной безопасности. Атаки, принципы и подходы	**7**	Поиск и метод исследования
3	1	Наиболее распространенные опасности. Защита данных и конфиденциальности	**7**	Поиск и метод исследования
4	1	Законодательный уровень информационной безопасности. Защита организации	**7**	Поиск и метод исследования
5	1	Стандарты и спецификации в области информационной безопасности. Законодательные и этические вопросы, образование и карьера в области кибербезопасности	**7**	Поиск и метод исследования
6	1	Административный уровень информационной безопасности. Кибербезопасность-мир экспертов и преступников	**7**	Поиск и метод исследования
7	1	Управление рисками. Куб кибербезопасности	**7**	Поиск и метод исследования
8	1	Процедурный уровень информационной безопасности. Кибербезопасность, уязвимости и атаки	**7**	Поиск и метод исследования
9	2	Основные программно-технические мероприятия. Способы защиты конфиденциальной информации	**7**	Поиск и метод исследования
10	2	Идентификация и аутентификация, контроль доступа. Искусство обеспечения целостности данных	**7**	Поиск и метод исследования
11	2	Протоколирование и аудит, шифрование, контроль целостности. Концепция "пять девять"	**7**	Поиск и метод исследования
12	2	Экранизация, анализ защиты. Защита уровней обеспечения кибербезопасности	**7**	Поиск и метод исследования
13	2	Обеспечение высокой доступности	**7**	Поиск и метод исследования
14	2	Туннелирование и управление	**7**	Поиск и метод исследования

15	2	Важность и сложность проблемы информационной безопасности	7	Поиск и метод исследования
		ИТОГО	**105**	

5. Краткая организационно-методическая характеристика дисциплины

Виды контроля учебных достижений:

Рубежный контроль: 1 устный

Рубежный контроль: 2 устный

***Итоговый контроль:* матричный тест**

(Формы текущего и рубежного контроля определяется преподавателем)

(Форма итогового контроля определяется кафедрой)

Альтернатива формы экзамена для обучающихся с особыми образовательными потребностями: Подготовка и защита проекта

Политика и процедуры курса:

- Обязательное посещение обучающимися всех занятий согласно расписанию;
- Предварительная подготовка к занятиям;
- Своевременное выполнение и сдача СРО;
-Подготовка ко всем видам занятий должна нести самостоятельный, творческий характер;
- Активная работа и проявление креативности во время занятий;
- Участие во всех видах контроля;
- Приверженность Политике академической честности университета.

Для студентов с особыми образовательными потребностями:

Учебные материалы предоставляются в упрощённом формате (увеличенный шрифт, аудиоверсия и др.); предоставляется дополнительное время на выполнение заданий; предлагаются альтернативные виды заданий; оказывается индивидуальное консультирование и поддержка.

Для удобства студентов предусмотрена гибкость участия — как в онлайн, так и в офлайн-формате. В случае пропуска занятий по медицинским или другим уважительным причинам — материал восполняется по индивидуальному графику.

Учебно-методическая обеспеченность дисциплины

№ п/п	Автор, наименование, издательство, год издания	Носитель информации.	Имеется в наличии (шт.)		
			В библиотеке	Мировые цифровые библиотеки	На кафедре
1	2	3	4		5
Основная литература					
1.	Интеллектуальные сервисы по управлению информацией и событиями безопасности в компьютерных системах и сетях : учебное пособие / А.Ж. Абденов. - Алматы : Эпиграф, 2019. - 149, [1] с. : ил., табл. - Библиогр.: с. 140-146. - ISBN 978-601-327-530-7.	Учебное пособие	50	https://library.enu.kz/MegaPro/Web/SearchResult/ToPage/1	
2.	Information and communication technologies. In 2 parts = Информационно-	Учебник	48	https://library.enu.kz/MegaPro/Web/SearchResult/ToPage/1	

	коммуникационные технологии : textbook. Part 2 / Republic of Kazakhstan, Ministry of education and science, International information technology university; D. Shynybekov, R. Uskenbayeva, V. Serbin, N. Duzbayev, A. Moldagulova, K. Duysebekova, R. Satybaldiyeva, G. Khasenova, B. Urmashev . - 1st ed. - Almaty : IITU, 2017. - 622, [1] с. : ил. - Библиогр. в конце гл. - ISBN 978-601-7911-04-1. - ISBN 978-6017911-02-7.				
3.	Information and communication technologies : tutorial / V.V. Yavorskiy, A.O. Chvanova, E.G. Klyueva. - Almaty : Эверо, 2021. - 182, [1] с. : ил. - Библиогр.: с. 182. - ISBN 978-601-342-582-5.	учебное пособие	30	https://library.enu.kz/MegaPro/Web/SearchResult/ToPage/1	
4.	Информационно-коммуникационные технологии : учебное пособие / Т.Б. Нурпеисова, И. Н. Кайдаш. - Алматы : Бастау, 2017. - 539, [1] с. : табл., ил. - Библиогр.: с. 534-539. - ISBN 978-601-281-230-5.	учебное пособие	100	https://library.enu.kz/MegaPro/Web/SearchResult/ToPage/1	
5.	Грушо А.А. Теоретические основы компьютерной безопасности : учебное пособие для студентов вузов / А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. - Москва : Академия, 2019. - 267, [2] с. - Библиогр.: с. 261-263. - ISBN 978-5-7695-4242-8.	Учебное пособие	+	https://library.enu.kz:443/MegaPro/UserEntry?Action=Link_FindDoc&id=169529&idb=0	
Дополнительная литература					
6.	Аудит безопасности информационных систем / Н.В. Скабцов. - Санкт-Петербург : Питер, 2018. - 268, [1] с. : ил. - (Библиотека программиста). - ISBN 978-5-4461-0662-2	Монография	23	https://library.enu.kz:443/MegaPro/UserEntry?Action=Link_FindDoc&id=170012&idb=0	
7.	Криптографическая защита информации : учебное пособие / П.С. Шевчук, С.В. Соколов, С.О. Крамаров [и др.] ; под редакцией С.О. Крамарова. - Москва : РИОР : ИНФРА-М, 2024. - 319, [2] с. : ил., табл. - (Высшее образование). - Библиогр.: с. 312-	Учебное пособие	20	https://library.enu.kz/MegaPro/UserEntry?Action=Link_FindDoc&id=171210&idb=0	

	315. - ISBN 978-5-369-01716-6. - ISBN 978-5-16-013274-7. - ISBN 978-5-16-106001-8				

7. Система оценки результатов учебных достижений обучающихся

Знания, умения и навыки студентов оцениваются по следующей системе

Оценка по буквенной системе	Цифровой эквивалент баллов	%-ное содержание	Оценка по традиционной системе	Критерии выставления
A	4,0	95-100	Отлично	Оценка **A** ставится в том случае, когда по дисциплине «Основы кибербезопасности» дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающихся.
A-	3,67	90-94		Оценка **A-** ставится в том случае, когда по дисциплине «Основы кибербезопасности» дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочеты в определении понятий, исправленные обучающимся самостоятельно в процессе ответа.
B+	3,33	85-89	Хорошо	Оценка **B+** ставится в том случае, когда обучающимся по дисциплине «Основы кибербезопасности» дан полный, развернутый ответ на поставленный вопрос, доказательно раскрыты основные положения темы в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Ответ изложен литературным языком в терминах науки. В ответе допущены недочеты, исправленные обучающимся с помощью преподавателя.
B	3,0	80-84		Оценка **B** ставится в том случае, когда по дисциплине «Основы кибербезопасности» дан полный, развернутый ответ на поставленный вопрос, показано умение выделить

				существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком в терминах науки. Могут быть допущены недочеты или незначительные ошибки, исправленные обучающимся с помощью преподавателя.
B-	2,67	75-79		Оценка **B-** ставится в том случае, когда по дисциплине «Основы кибербезопасности» дан развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки. Однако допущены незначительные ошибки или недочеты, исправленные обучающимся с помощью наводящих вопросов.
C+	2,33	70-74		Оценка **C+** ставится в том случае, когда по дисциплине «Основы кибербезопасности» дан полный, но недостаточно последовательный ответ на поставленный вопрос, но при этом показано умение выделить существенные и несущественные признаки и причинно-следственные связи. Ответ логичен и изложен в терминах науки. Могут быть допущены 1–2 ошибки в определении основных понятий, которые обучающийся затруднился исправить самостоятельно.
C	2,0	65-69	Удовлетворительно	Оценка **C** ставится в том случае, когда по дисциплине «Основы кибербезопасности» дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Обучающийся не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Обучающийся может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции.
C-	1,67	60-64		Оценка **C-** ставится в том случае, когда по дисциплине «Основы кибербезопасности» дан неполный ответ, логика, и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания обучающимся их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.
D+	1,33	55-59		Оценка **D+** ставится в том случае, когда по дисциплине «Основы кибербезопасности» дан неполный ответ. Присутствует нелогичность

				изложения. Обучающий затрудняется с доказательностью. Масса существенных ошибок в определениях терминов, понятий, характеристике фактов, явлений. В ответе отсутствуют вводы. Речь неграмотна. При ответе на дополнительные вопросы Обучающий начинает осознавать существование связи между знаниями только после подсказки преподавателя.
D	1,0	50-54		Оценка **D** ставится в том случае, когда по дисциплине «Основы кибербезопасности» дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Обучающий не осознает связь данного понятия, теории, явления с другими объектами модуля (дисциплины). Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа обучающегося не только на поставленный вопрос, но и на другие вопросы модуля (дисциплины).
FX	0,5	25-49	Неудовлетворительно	Оценке «неудовлетворительно» соответствует буква **FX, F,** имеющая цифровой эквивалент 0 и процентное содержание 0-49. Данная оценка ставится в том случае, если обучающийся по дисциплине «Основы кибербезопасности» обнаружил пробелы в знании основного материала, предусмотренного программой, не освоил более половины программы модуля (дисциплины), в ответах допустил принципиальные ошибки, не выполнил отдельные задания, предусмотренные формами текущего, промежуточного и итогового контроля, не проработал всю основную литературу, предусмотренную программой.
F	0	0-24		