Алматинский гуманитарно-экономический университет

Кафедра «ИСиООД»

«ОДОБРЕНО на УМС АГЭУ»
Первый проректор АГЭУ
к.э.н., профессор Бекенова Л.М.
« 28 » августа 2023 г.

УЧЕБНАЯ ПРОГРАММА ДИСЦИПЛИНЫ (СИЛЛАБУС

дисциплины «Современная криптология»
Группа образовательных программ: Информационные технологии (М094)
По образовательной программе: 7М06121- «Информационные системы»

1	**Код и наименование дисциплины**	SK 5207
2	**Цикл, компонент**	БД/КВ
3	**Всего кредитов**	5
4	**Курс**	1
5	**Семестр**	2
6	**Экзамен (семестр)**	2
7	**Всего часов, из них:**	150
8	**Лекции (часов)**	30
9	**Практические (семинарские) занятия (часов)**	15
10	**СРСП (часов)**	45
12	**СРС (часов)**	60
13	**Форма и платформа итогового контроля**	Тест, СДО Прометей
14	**Преподаватель**	Байсалбаева К.Н.
15	**e-mail:**	k.bais@mail.ru
16	**Телефон:**	8 707 335 0775

Алматы, 2023 г

АКАДЕМИЧЕСКАЯ ПРЕЗЕНТАЦИЯ ДИСЦИПЛИНЫ	
Актуальность и краткое содержание дисципилины	Дисциплина«Современная криптология»посвящен изучению современных концепций информационной безопасности и их применения в обеспечении защиты информации и безопасного использования программных средств в вычислительных системах.
Ожидаемые результаты обучения (РО)*	Цель изучения дисциплины: Цель курса – научить магистра методам информационной безопасности и их использовании в области защиты информации. Воспитательной целью дисциплины является формирование у магистров научного, творческого подхода к освоению технологий, методов и средств производства и защиты программного обеспечения. Дать магистрам математические основы защиты информации.
	1.**РО6:**Планировать, проектировать, а также использовать цифровые технологии во всех сферах предпринимательской деятельности, оценивать эффективность цифровой трансформации, выявлять и анализировать проблемы цифровизации, учитывать самые современные технологии.
Цель дисциплины:	В результате изучения учебной дисциплины магистрант магистратуры должен: **знать:** –наиболее известные криптографические функции хеширования; –основные симметричные и асимметричные криптосистемы; –стандарты электронной цифровой подписи; **уметь:** –корректно применять основные криптосистемы, функции хеширования; –формировать электронную цифровую подпись под электронным документом; –видеть в криптографических протоколах применяемые свойства математических объектов; **владеть:** –навыками исследования сложных криптографических систем; –методами обеспечения целостности и аутентификации информации
Пререквизиты	Технология разработки управленческих решений
Постреквизиты	Корпоративные информационные системы
Основная и дополнительнаялитература	**Основная литература:** **1.** Харин, Ю.С. Математические основы теории информации: учеб.пособие для студ. учреждений высш. образования по спец. "Компьютерная безопасность", "Прикладная криптография" / Ю. С.Харин, И. А. Бодягин, Е. В. Вечерко; БГУ. - Минск: БГУ, 2018. 2. Авдошин, С.М. Дискретная математика. Модулярная алгебра, криптография, кодирование / С. М. Авдошин, А. А. Набебин; [науч.ред. В. А. Захаров]. - Москва: ДМК Пресс, 2017. 3. Бабаш, А.В. Криптографические методы защиты информации: учебник для студ. вузов, обуч. по напр. "Прикладная информатика" / А. В. Бабаш, Е. К. Баранова. - Москва: КНОРУС, 2016. 4. PKCS#1 v2.2: RSA Cryptography Standart [Electronic resource]. RSALaboratories, 2012. – Mode of access: https://www.emc.com/ collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-

	standardwp.pdf. – Date of access: 02.04.2020. 5.Digital Signature Standard (DSS) // Federal information processing standards publication [Electronic resource]. National Institute of Standards and Technology, 2013. – Mode of access: http://dx.doi.org/10.6028/NIST.FIPS.186-4.pdf. – Date of access: 02.04.2020. 6.О развитии цифровой экономики. Декрет № 8 от 21 декабря 2017 г.[Электронный ресурс]. – Режим доступа: http://president.gov.by/uploads/archives/Decret-8.zip – Дата доступа:03.02.2020. 7.Введение в смарт-контракты [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/distributedlab/blog/413231/ – Дата доступа: 03.02.2020. 8.Официальный сайт криптовалютыЭфириум [Электронный ресурс]. –Режим доступа: https://www.ethereum.org/ – Дата доступа: 02.04.2020. 9.Opensource [Электронный ресурс]. – Режим доступа: https://github.com/ethereum/trinity – Дата доступа: 02.04.2020. 10.Bitcoin Developer Reference. [Electronic resource]. – Mode of access:https://bitcoin.org/en/developer-reference#block-chain – Date of access:02.04.2020. 11.Bitcoin Core. [Electronic resource]. – Mode of access: https://github.com/bitcoin/bitcoin – Date of access: 02.04.2020. **Дополнительнаялитература:** 1.Нестеренко, Ю.В. Теория чисел: учебник для студ. высш. учеб. заведений / Ю.В. Нестеренко. – М.: Издательский центр «Академия», 2008. – 272 с 2. ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017 3. Информационная безопасность : учебное пособие для магистрантов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017
Академическая политика дисциплины	Академическая политика дисциплины определяется Политикой академической честности АГЭУ. *Документы доступны на сайтеageu.edu.kz в разделевнутренниедокументы*. **Академическая честность:** совокупность; ценностей и принципов, выражающих честность обучающихся в обучении при выполнении письменных работ (контрольных, курсовых, эссе, дипломных, диссертационных), ответах на экзаменах, (в исследованиях, выражении своей позиции, в взаимоотношениях

	с академическим персоналом, преподавателями и другими обучающимися, а также оценивании). *Документы доступны на сайтеageu.edu.kz в разделевнутренниедокументы*. **Требованияпредъявляемыемагистрантам:** — не опаздывать на занятия, обязательность посещения занятий и не допустимость пропуска занятий без уважительной причины; — опоздание на занятия (лекционные или занятия другой формы) опоздание в количестве два раза приравнивается к пропуску одного занятия; — магистрант должен письменно фиксировать основные моменты текста лекций; — активно участвовать в учебном процессе; — выполнять домашние задания, приходить подготовленным к практическим и прочим занятиям; — задания выполнять и сдавать в установленные сроки, если задание предоставляется после установленного срока, преподаватель имеет право отказать в приеме задания; — при сдаче тестов не разрешаются помарки и исправления в обозначении ответов на тестовые вопросы; — магистрант обязан владеть терминами по изучаемому курсу; — озапрещается пользоваться мобильными телефонами во время занятий; — опри подготовке к занятиям в форме дискуссий, магистр должны владеть материалом и полностью раскрыть суть поставленного вопроса.

ИНФОРМАЦИЯ ОБ ОЦЕНИВАНИИ

<table>
<tr><th colspan="4">Балльно-рейтинговая буквенная система оценки учета учебных достижений</th><th rowspan="2">Методы оценивания</th></tr>
<tr><th>Оценка</th><th>Цифровой эквивалент баллов</th><th>Баллы, % содержание</th><th>Оценка по традиционной системе</th></tr>
<tr><td>A</td><td>4,0</td><td>95-100</td><td rowspan="2">Отлично</td><td rowspan="4">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,</td></tr>
<tr><td>A-</td><td>3,67</td><td>90-94</td></tr>
<tr><td>B+</td><td>3,33</td><td>85-89</td><td>Хорошо</td></tr>
</table>

				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 СРС.Это оценивание освоения ожидаемых результатов обучения в соотнесенности с дескрипторами. Позволяет определять и фиксировать уровень освоения дисциплины за определенный период. Оцениваются результаты обучения.	
B	3,0	80-84		**Формативное и суммативное оценивание** Преподаватель вносит свои виды оценивания либо использует предложенный вариант	**Баллы % содержание** Преподаватель вносит свою разбалловку в пункты в соответствии с календарем (графиком). Не изменяются экзамен и итоговый балл по дисциплине.
B-	2,67	75-79			
C+	2,33	70-74		Работа на практических занятиях	30
C	2,0	65-69	Удовлетворительно	Самостоятельная работа	30
C-	1,67	60-64			
D+	1,33	55-59	Неудовлетворительно	Итоговый контроль (экзамен)	40
D	1,0	50-54		ИТОГО	100

Типовые критерии оценки показателей успеваемости магистранта по дисциплине	
Степень успеваемости магистранта по дисциплине (степень знания, квалификации и навыков)	***Баллы***
Магистрант имеет достаточно глубокие знания по темам дисциплины, понимает их сущность, на основе самостоятельно полученных знаний из дополнительно изученных литератур, делает выводы и принимает правильные решения как на теоретических, так и практических занятиях, свои ответы обосновывает практическими (условными) примерами и теоретическими данными. Может самостоятельно размышлять над поставленным заданием, принимать решения и обосновывать их, а также применять их на практике.	*86-100 балл*
Магистрант имеет понятие по темам дисциплины, понимает их	*71-85 балл*

сущность, делает выводы и принимает правильные решения, свои ответы обосновывает практическими (условными) примерами и теоретическими данными.	
Магистрант имеет удовлетворительные понятие о темах дисциплины, понимает их сущность, делает выводы и принимает правильные решения, при этом в своих ответах полностью не раскрывает сущность теоретических вопросов и допускает ошибки при решении.	*55-70 балл*
Магистрант не имеет понятия о темах дисциплины, не представляет их сущность, заблуждается неверными выводами и решениями в своих ответах, при этом не может решить задачи.	*0-54 балл*

Система оценки знаний магистранта

Оценки по текущей успеваемости складываются из оценок текущего контроля и рубежного (промежуточного) контроля.

Текущий контроль успеваемости – систематическая проверка учебных достижений магистранта по каждой теме учебной дисциплины, проводимая преподавателем, ведущим учебное занятие.

Рубежный контроль проводится по завершении изучения крупных разделов (модулей) учебной дисциплины.

Итоговая оценка по дисциплине включает оценки текущей успеваемости и итогового контроля. Оценка текущей успеваемости (рейтинг допуска) составляет 60% от итоговой оценки знаний по дисциплине. Оценка экзамена составляет 40% от итоговой оценки знаний по дисциплине.

Оценка знаний магистранта осуществляется по балльно-рейтинговой буквенной системе с соответствующим переводом в традиционную шкалу оценок.

Расчет итоговой оценки

Итоговая оценка по дисциплинев процентном содержании определяется по следующей формуле:

$$И\% = \frac{Р1+Р2}{2} \times 0,6 + Э \times 0,4$$

где:

Р1 – процентное содержание оценки 1-го рейтинга;

Р2 – процентное содержание оценки 2-го рейтинга;

Э – процентное содержание экзаменационной оценки (тест-экзамен).

Календарно-тематический план дисциплины

п/п	Название темы	**Учебные часы**				
		Всего	**Лекции**	**Практи чес. занятия**	**СРСП**	**СРС**
1	Базовые понятия и история развития информационной безопасности.					
2	Криптографические функции хеширования. История, обзор актуальных криптографических функций хеширования.	10	2	1	3	4

3	Шифры замены. Шифры перестановки. Шифры гаммирования.	10	2	1	3	4
4	Криптосистема AES. Алгоритмы шифрования и расшифрования AES. Криптоанализ AES.	10				4
5	Криптосистема RSA. Криптосистемы с открытым ключом. Криптосистема RSA.	10	2	1	3	4
6	Электронная цифровая подпись. Стандарты подписи на основе мультипликативной группы кольца вычетов: DSA, СТБ1176.2 – 99, ГОСТ3410 - 94.	10	2	1	3	4
7	Эллиптические кривые. Группа точек эллиптической кривой. Порядок группы, алгоритм Шуфа.	10	2	1	3	4
8	Электронная цифровая подпись на основе группы точек эллиптической кривой.	10	2	1	3	4
9	КриптовалютаБиткоин. Назначение криптовалютыБиткоин. Цепочка блоков. М	10	2	1	3	4
10	КриптовалютаЭфириум. Назначение криптовалютыЭфириум.	10	2	1	3	4
11	Системы электронного голосования. ElectionGuard. Гомоморфные шифры. Криптосистема Эль-Гамаля в экспоненциальной форме.	10	2	1	3	4
12	Мессенджеры. Мессенджер Telegram. Алгоритм регистрации.	10	2	1	3	4
13	Цифровые водяные знаки. Стеганография. Свойства цифровых водяных знаков. Классификация. Применение.	10	2	1	3	4
14	Блочные системы шифрования. ,. Принципы построения блочных шифров.	10	2	1	3	4
15	Поточные системы шифрования. Шифрсистема А5. ШифрсистемаГиффорда.	10	2	1	3	4
	Итого:	**150**	**30**	**15**	**45**	**60**

План лекции, практических (семинарских)		
№	**Тематика лекций**	**План лабораторных занятий**

1	Базовые понятия и история развития информационной безопасности.	Основные шифры
2	Криптографические функции хеширования. Криптографические функции хеширования. История, обзор актуальных криптографических функций хеширования. MD5, SHA-1, SHA-2, SHA-3, их реализация и криптостойкость. Атаки на MD5. Атака SHAttered.	Стойкость шифров.
3	Шифры замены. Шифры перестановки. Шифры гаммирования.	Конечные поля. Характеристика поля. Мультипликативная группа конечного поля
4	Криптосистема AES. Алгоритмы шифрования и расшифрования AES. Алгебраическое представление AES. Криптоанализ AES. Способы дополнения сообщений. Режимы сцепления блоков шифротекста.	Неприводимые многочлены. Порядок многочлена над конечным полем. Последовательности над конечным полем.
5	Криптосистема RSA. Криптосистемы с открытым ключом. Криптосистема RSA. Криптоанализ RSA. Стандарт PKCS#1. Методы преобразования сообщения: PKCS, OAEP. Криптосистема RSA с модулем, являющимся произведением более двух простых чисел.	Математическая модель шифра замены. Поточные шифры простой замены. Блочные шифры простой замены.
6	Электронная цифровая подпись. Электронная цифровая подпись. Стандарты подписи на основе мультипликативной группы кольца вычетов: DSA, СТБ1176.2 – 99, ГОСТ3410 - 94.	Многоалфавитные шифры замены. Шифры перестановки. Маршрутные перестановки.
	Эллиптические кривые. Группа точек эллиптической кривой. Порядок группы, алгоритм Шуфа. Криптосистемы на основе группы точек эллиптической кривой.	Табличное гаммирование.
7	Электронная цифровая подпись на основе группы точек эллиптической кривой. Электронная цифровая подпись. Стандарты электронной цифровой подписи на основе группы точек эллиптической кривой: СТБ 34.101.45-2013, ГОСТ Р 34.10-2012, ECDSA.	Принципы построения блочных шифров.
8	КриптовалютаБиткоин. Назначение криптовалютыБиткоин. Цепочка блоков. Майнинг. Доказательство работой. Содержимое блока, транзакция, адрес. Эллиптическая кривая Secp256k1.	Американский стандарт шифрования данных DES и его модификации.
9	КриптовалютаЭфириум. Назначение криптовалютыЭфириум. Цепочка блоков. Майнинг. Доказательство работой и доказательство владением. Содержимое блока, транзакция, адрес, учетные записи. Смарт-контракты. Декрет Президента Республики Беларусь № 8.	Стандарт шифрования данных ГОСТ 28147-89. Методы анализа алгоритмов блочного шифрования
10	Системы электронного голосования. 6 Система электронного голосования ElectionGuard. Гомоморфные шифры. Криптосистема Эль-Гамаля в экспоненциальной форме. Доказательство с нулевым разглашением. Разделение секрета. Системы сквозного проверяемого голосования. Проверка	Цифровые подписи. Одноразовые цифровые подписи.

	подсчета всех голосов. Возможность избирателя проверить включение своего голоса в итоговый подсчет. Невозможность продажи голосов. Невозможность вброса бюллетеней	
11	Мессенджеры. Мессенджер Telegram. Алгоритм регистрации. Протокол MTProto. Атака «человек посередине» во время регистрации. Атака «человек посередине» во время сквозного шифрования.	Идентификация. Фиксированные пароли. Парольные фразы.
12	Цифровые водяные знаки. Стеганография. Цифровой водяной знак. Свойства цифровых водяных знаков. Классификация. Применение. Цифровые водяные знаки на основе сингулярного разложения.	Линейные регистры сдвига.
13	Блочные системы шифрования. , Блочные системы шифрования. Принципы построения блочных шифров. Американский стандарт шифрования данных DES. Стандарт шифрования данных ГОСТ 28147-89. Методы анализа алгоритмов блочного шифрования	Стандарт шифрования данных ГОСТ 28147-89. Методы анализа алгоритмов блочного шифрования
14	Поточные системы шифрования. Поточные системы шифрования. Шифрсистема А5. ШифрсистемаГиффорда. Линейные регистры собеседование, индивидуальное 8 сдвига. Алгоритм Берлекемпа—Месси. Методы анализа поточных шифров.	Поточные системы шифрования.
15	Базовые понятия и история развития информационной безопасности.	Методы анализа поточных шифров.

Самостоятельная работа магистрантовпод руководством преподавателя

№	**Наименование тем и содержание заданийдля СРСП**	**Формы проведения**	**Объем в часах**	**Неделя семестра**
1	Базовые понятия и история развития информационной безопасности.	Работа с учебниками подготовка конспектов. Проблемно-проектная дискуссия	1	1
2	Криптографические функции хеширования. История, обзор актуальных криптографических функций хеширования.	Подготовить письменные ответы	1	2
3	Шифры замены. Шифры перестановки. Шифры гаммирования.	Письменная работа	1	3
4	Криптосистема AES. Алгоритмы шифрования и расшифрования AES. Криптоанализ AES.	Письменная работа	1	4
5	Криптосистема RSA. Криптосистемы с открытым ключом. Криптосистема RSA.	Письменная работа	1	5
6	Электронная цифровая подпись. Стандарты подписи на основе мультипликативной группы кольца вычетов: DSA, СТБ1176.2 – 99, ГОСТ3410 - 94.	Письменная работа	1	6

7	Эллиптические кривые. Группа точек эллиптической кривой. Порядок группы, алгоритм Шуфа.	Письменная работа	1	7
8	Электронная цифровая подпись на основе группы точек эллиптической кривой.	Подготовить конспект, провести сравнительный анализ.	1	8
9	КриптовалютаБиткоин. Назначение криптовалютыБиткоин. Цепочка блоков. М	Подготовить доклады по заданным темам	1	9
10	КриптовалютаЭфириум. Назначение криптовалютыЭфириум.	Письменная работа	1	10
11	Системы электронного голосования. ElectionGuard. Гомоморфные шифры. Криптосистема Эль-Гамаля в экспоненциальной форме.	Письменная работа	1	11
12	Мессенджеры. Мессенджер Telegram. Алгоритм регистрации.	Письменная работа	1	12
13	Цифровые водяные знаки. Стеганография. Свойства цифровых водяных знаков. Классификация. Применение.	Письменная работа	1	13
14	Блочные системы шифрования. ,. Принципы построения блочных шифров.	Письменная работа	1	14
15	Поточные системы шифрования. Шифрсистема А5. ШифрсистемаГиффорда.	Письменная работа	1	15
	Всего:		**15**	**15**

Самостоятельная работа магистрантов

№ №	**Наименование тем и содержание заданий для СРС**	**Форма контроля**	**Объем в часах**	**Неделя семестра**
1	Криптосистема RSA. Криптосистемы с открытым ключом. Криптосистема RSA. Криптоанализ RSA. Стандарт PKCS#1. Методы преобразования сообщения: PKCS, OAEP. Криптосистема RSA с модулем, являющимся произведением более двух простых чисел.	Проверка работы. Оформленный отчет.	20	3 неделя
2	Электронная цифровая подпись. Электронная цифровая подпись. Стандарты подписи на основе мультипликативной группы кольца вычетов: DSA, СТБ1176.2 – 99, ГОСТ3410 - 94.	Проверка работы. Оформленный отчет.	20	7неделя
3	Блочные системы шифрования. , Блочные системы шифрования. Принципы построения блочных шифров. Американский стандарт шифрования данных DES. Стандарт	Проверка работы. Оформленный отчет.	20	12 неделя

	шифрования данных ГОСТ 28147-89. Методы анализа алгоритмов блочного шифрования			

Одобрено на заседании кафедры "ИС и ООД"
Протокол № __ от "___" _____ 2023г

И.О.зав.кафедрой "ИС и ООД" стар.преподаватель _____ Иембердиева Б.Н. Иембердиева Б.Н.

PhD, доцент кафедры «ИСиООД» _____ Байсалб