СИЛЛАБУС
Осенний семестр 2024–2025 уч. год
Образовательная программа «6B03208 – Цифровое архивоведение и документоведение»

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)**		
ID 21121 Информационная безопасность и защита информации	6	3,0	3,0	3,0	9	7

АКАДЕМИЧЕСКАЯ ИНФОРМАЦИЯ О ДИСЦИПЛИНЕ

Формат обучения	**Цикл, модуль компонент**	**Типы лекций**	**Типы практических занятий**	**Форма и платформа итогового контроля**
Офлайн обучение	ПД ВК	Информационная лекция, проблемная лекция, лекция-конференция, лекция-консультация, лекция-визуализация.	Семинар-беседа, семинар «мозговой штурм», семинар-диспут, семинар-дискуссия, семинар «деловая игра», смешанная форма семинара с решением ситуационных задач, по моделированию реальных задач, семинар-имитация	Письменный
Лектор - (ы)	Жакишева Сауле Аукеновна			
e-mail:	adiconilau@mail.ru			
Телефон:	377 33 38 (вн. 1289) +7 7017634995			
Ассистент- (ы)	Ходжабай Мухтар			
e-mail:	mukhtar@kazrena.kz			
Телефон:	377 33 38 (вн. 1289) +7 7715518558			

АКАДЕМИЧЕСКАЯ ПРЕЗЕНТАЦИЯ ДИСЦИПЛИНЫ

Цель дисциплины	**Ожидаемые результаты обучения (РО)** В результате изучения дисциплины обучающийся будет способен:	**Индикаторы достижения РО (ИД)** (на каждый РО не менее 2-х индикаторов)
Цель дисциплины сформировать способность понимать сущность и значение информации в развитии современного информационного общества. Дисциплина направлена на изучение: состава защищаемой информации, структуры угроз информации видов и методов деятельности по обеспечению информационной безопасности, основы правового и организационного обеспечения информационной безопасности, классификации информационной безопасности, анализа методов и средств защиты информации.	**РО 1** - использовать основы правовых знаний в области защиты информационных ресурсов на уровне их воспроизведения.	**ИП 1.1** – понимает смысл, воспроизводит и использует нормативно-правовые акты в сфере информационной безопасности, дает законодательно и нормативно установленные определения базовым понятиям «конфиденциальный документ», «документированная информация» **ИД 1.2** - - использует нормативно-правовые акты, регламентирующие организацию работы с документами, содержащими коммерческую тайну. **ИД 1.3** – воспроизводит и применяет законодательные нормативно-правовые акты в сфере организации работы с документами, содержащими информацию ограниченного доступа. **ИД 1.4** – иллюстрирует применимость норм и стандартов ИСО в области информационной

		безопасности и защиты информации в РК.
	РО 2 – использовать основные методы, способы и средства получения, хранения, переработки информации	**ИД 2.1** – определяет источники конфиденциальной информации, методы, способы и средства ее получения, хранения и переработки. **ИД 2.2** – воспроизводит правила разработки и организации работы с документами, составляющими коммерческую тайну. **ИД 2.3** – анализирует и использует нормативно-правовые акты в сфере организации работы с документами, содержащими информацию ограниченного доступа.
	РО 3 – анализировать и использовать методы защиты информации.	**ИД 3.1** – знает структуру и методы защиты информации. **ИД 3.2** – определяет правила текущей работы и особенности увольнения сотрудников, владеющих конфиденциальной информацией. **ИД 3.3** – использует технологические системы защиты и обработки конфиденциальных документов. **ИД 3.4 –** учитывает в практической работе **о**собенности составления и ведения номенклатуры конфиденциальных дел, порядок уничтожения документов, дел и носителей информации.
	РО 4 – оценивать и обобщать приемы, методы, методики и технологии информационной безопасности и защиты информации	**ИД 4.1 -** различает специфику, особенности и ограничения технологий информационной безопасности и защиты информации. **ИД 4.2** – определяет различные подходы в реализации целей и задач информационной безопасности и защиты информации. **ИД 4.3 –** решает организационно-управленческие задачи в области информационной безопасности и защиты информации. **ИД 4.4 –** определяет и обосновывает необходимость развития дальнейшего совершенствования методов и методик работы с конфиденциальной информацией с учетом международного опыта в этой сфере.
	РО 5 – проводить различия в реализации задач информационной безопасности и защиты информации в РК и за рубежом	**ИД 5.1** – выбирать и применять методы, способы и средства получения, хранения и переработки конфиденциальной информации в контексте защиты персональных данных. **ИД 5.2** – выбирать и применять методы защиты информации в сетевых и локальных системах. **ИД 5.3** – воспроизводить правила разработки и организации работы с документами, составляющими коммерческую тайну.
Пререквизиты	Информационно-коммуникационные технологии [89242]; Обеспечение сохранности архивных документов [91530]	
Постреквизиты	Автоматизированные архивные технологии [72919]; Информационные технологии в документационном обеспечении управлении [64344]	
Литература и ресурсы	**Литература:** 1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов. – М.: ФЛИНТА, 2011. - 184 с. - Режим доступа: http://www.knigafund.ru. 2. Прохорова О. В. Информационная безопасность и защита информации: учебник для СПО / О. В. Прохорова. – 2-е изд., стер. – СПб: Лань, 2021. – 124 с. 3. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория	

	информационной безопасности и методология защиты информации. 2-е изд., испр. и доп. – СПб.: Университет ИТМО, 2018. – 100 с. 4. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е. К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с. 5. Краковский, Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. - РнД: Феникс, 2017. - 347 с. 6. Крамаров, С.О. Криптографическая защита информации: Учебное пособие / С.О. Крамаров, Е.Н. Тищенко, С.В. Соколов и др. - М.: Риор, 2019. - 112 с. 7. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. - 230 с. 8. Мельников, В.П. Защита информации: Учебник / В.П. Мельников. - М.: Академия, 2019. - 320 с. **Источники:** 1. Закон РК «О национальном архивном фонде и архивах» от 22 декабря 1998 г. №326–1. 2. Закон РК «Об информатизации» от 24 ноября 2015 г. № 418-V ЗРК. 3. Закон РК «Об электронном документе и электронной цифровой подписи» от 7 января 2003 года №370. 4. «Ұлттық архив қорының құжаттарын және басқа да архивтік құжаттарды мемлекеттік және арнаулы мемлекеттік архивтердің жинақтау, сақтау, есепке алу мен пайдалану қағидаларын бекіту туралы Қазақстан Республикасы Үкіметінің 2018 жылғы 20 қыркүйектегі № 576 қаулысы 5. «Ұлттық архив қорының құжаттарын және басқа да архивтік құжаттарды ведомстволық және жеке архивтердің қабылдау, сақтау, есепке алу мен пайдалану қағидалары туралы» Қазақстан Республикасы Үкметінің 2018 жылғы 19 қыркүйектегі № 575 қаулысы 6. СТ РК ISO 19005-1-2016 «Управление документацией. Формат файлов электронных документов для долгосрочного хранения. Часть 1. Использование PDF 1.4 (PDF/A-1)» **Исследовательская инфраструктура** Аудитория с передвижным интерактивным дисплеем. **Профессиональные научные базы данных:** 1. Scopus: URL: https://www.elsevier.com/products/scopus 2. Web of Science. URL: https://www.webofscience.com/ 3. РИНЦ. eLIBRARY.ru Российская электронная библиотека научных публикаций. URL: https://www.elibrary.ru/defaultx.asp 4. Академия Google URL: https://scholar.google.com/ 5. Science Direct. URL: https://www.sciencedirect.com/ 6. SpringerLink. Международная реферативная база данных научных изданий. URL: https://link.springer.com/ **Интернет-ресурсы:** ЗАЩИТА ИНФОРМАЦИИ И (narod.ru) http:// laleshin.narod.ru/l-ziib.htm Защита информации и информационная безопасность Алешин Л. 1. Сайт «International Organization for Standardization»: https://www.iso.org/structure.html. 2. Сайт Комитета технического регулирования и метрологии Министерства по инвестициям и развитию РК – Режим доступа: http://memst.mid.gov.kz /. 3. Сайт ppt-online.org. – Режим доступа: Информационная безопасность - презентация онлайн (ppt-online.org) 4. Интернет сайт Агентства РК по информатизации и связи - www.aic.gov.kz. **Интернет-ресурс КазНУ** 1. http://elibrary.kaznu.kz/ru
Академическая политика дисциплины	Академическая политика дисциплины определяется Академической политикой и Политикой академической честности КазНУ имени аль-Фараби. 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», «Инструкции для проведения итогового контроля осеннего/весеннего семестра текущего учебного года», «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/ e-mail adiconilau@mail.ru либо посредством видеосвязи в Zoom https://us04web.zoom.us/j/5632587811?pwd=VkRnSlQzNExwVEMxckh6UEpMekJrZz09 **Интеграция MOOC (massive open online course).** В случае интеграции МООС в дисциплину, всем обучающимся необходимо зарегистрироваться на МООС. Сроки прохождения модулей МООС должны неукоснительно соблюдаться в соответствии с графиком изучения дисциплины. **ВНИМАНИЕ!** Дедлайн каждого задания указан в календаре (графике) реализации содержания дисциплины, а также в МООС. Несоблюдение дедлайнов приводит к потере баллов.

ИНФОРМАЦИЯ О ПРЕПОДАВАНИИ, ОБУЧЕНИИ И ОЦЕНИВАНИИ

Балльно-рейтинговая буквенная система оценки учета учебных достижений

Оценка	Цифровой эквивалент баллов	Баллы, % содержание	Оценка по традиционной системе
A	4,0	95-100	Отлично
A-	3,67	90-94	
B+	3,33	85-89	Хорошо

Методы оценивания

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.	
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		Проектная и творческая деятельность	40
D	1,0	50-54		ИТОГО	100
FX	0,5	25-49			
F	0	0-24	Неудовлетворительно		

Календарь (график) реализации содержания дисциплины. Методы преподавания и обучения.

Неделя	**Название темы**	**Кол-во часов**	**Максимальный балл**
МОДУЛЬ 1. ВВЕДЕНИЕ В ПРЕДМЕТ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»			
1	**Л 1-2.** Безопасность в информационном обществе. Информационное общество как новый этап развития цивилизации.	2	
	СЗ 1–2. Решение задач на тему «Понятие ценных информационных ресурсов»	2	
	ЛЗ 1–2 Решение кейсов на тему «Понятие ценных информационных ресурсов»	2	
2	**ЛЗ-4.** Теория информационной безопасности. Информационная безопасность и ее составляющие. Информационная безопасность человека и общества.	2	
	СЗ 3–4. Решение задач на тему «Аналитическая работа при обеспечении информационной безопасности»	2	2
	ЛР 3-4. Решение кейсов на тему «Аналитическая работа при обеспечении информационной безопасности»	2	3
	СРОП 1. Консультации по выполнению **СРО 1**		
3	**Л 5-6.** Проблема безопасности в информационном обществе.	2	
	СЗ 5–6. Решение задач на тему: «Разработка и ведение перечня сведений, составляющих коммерческую тайну»	2	5
	ЛР5-2. Решение кейсов на тему «Разработка и ведение перечня сведений, составляющих коммерческую тайну»	2	5
	СРО 1. Решение проектного задания «История шпионажа и мероприятий по защите информации и сохранению государственной и коммерческой тайны». 1. Определить свойства информации: конфиденциальность; целостность, доступность. 2.Отметить понятие защищаемой информации и принципы отнесения к ней. 3. Классификация носителей защищаемой информации.		20
МОДУЛЬ 2. ХАРАКТЕРИСТИКА МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ			
4	**Л 7–8.** Классификация основных методов и средств защиты информации в центрах обработки, компьютерах и сетях	2	
	СЗ 7–8. Решение задачи на тему: «Технологические системы обработки и хранения конфиденциальных документов»	2	5
	ЛЗ 7–8. Решение кейсов на тему «Технологические системы обработки и хранения конфиденциальных документов»	2	5

	СРОП 2. Консультации по выполнению **СРО 2**		
5	**Л9-10.** Уровни и классы защиты информации	2	
	СЗ 9–10. Решение задачи на тему: «Порядок работы персонала с конфиденциальными документами»	2	5
	ЛЗ 9–10. Решение кейсов на тему «Порядок работы персонала с конфиденциальными документами»	2	5
	СРО 2. Решение аналитического задания на тему: «Понятие, сущность и цели защиты информации». 1. Описать понятие, сущность, цели и задачи защиты информации как деятельности. 2. Раскрыть виды защиты информации (правовая, техническая, криптографическая, физическая)		15
	СРОП 3. Консультации по выполнению **СРО 3**		
6	**Л 11–12.** Правовое обеспечение информационной безопасности. УК РК, организационно-распорядительные документы: Защита от несанкционированного доступа к информации. Термины и определения; Концепция защиты средств вычислительной техники и автоматизированных систем (АС) от несанкционированных действий (НСД) к информации; Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации; Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации.	2	
	СЗ 11–СЗ 12. Решение задач на тему: «Формирование конфиденциальных документов в дела, хранение дел и передача их в архив. Уничтожение документов, дел и носителей информации»	2	2
	ЛЗ 11–12. Решение кейсов на тему «Формирование конфиденциальных документов в дела, хранение дел и передача их в архив. Уничтожение документов, дел и носителей информации»	2	3
	СРО 3. Решение аналитического задания на тему: «Сетевая безопасность» 1. Описать угрозы сетевой безопасности, сущность, цели и задачи защиты своей сети 2. Типы сетевых атак 3. Описание других видов угроз сетевой безопасности. 4. Как защитить свою сеть?		20
7	**Л 13-14.**Технические средства охраны объектов	2	
	СЗ 13–СЗ 14. Решение задач на тему: «Организация работы с персоналом, обладающим конфиденциальной информацией»	2	2
	ЛЗ 13-ЛЗ 14. Решение кейсов на тему «Организация работы с персоналом, обладающим конфиденциальной информацией»	2	3
Рубежный контроль 1			**100**
МОДУЛЬ 3. НАПРАВЛЕНИЯ И ОТНОСЯЩИЕСЯ К НИМ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ			
8	**Л 15-16.** Технические средства противодействия съему информации по основным возможным каналам ее утечки	2	
	СЗ 15–16. Решение задач на тему: «Порядок проведения совещаний и переговоров по конфиденциальным вопросам, приема посетителей»	2	2
	ЛЗ 15–16. Решение кейсов на тему «Порядок проведения совещаний и переговоров по конфиденциальным вопросам, приема посетителей»	2	3
	СРОП 4. Консультации по выполнению **СРО4**		
9	**Л 17–18.** Место информационной безопасности в системе национальной безопасности РК	2	
	СЗ 17–18. Решение задач на тему: «Глобальная культура кибербезопасности».	2	2
	ЛЗ 17–18. Решение кейсов на тему: «Глобальная культура кибербезопасности».	2	3
	СРО 4. Проектное задание на тему: «Информационная война в системе международных отношений». 1. Раскрыть сущность информационной войны на современном этапе. 2. Проанализировать методы борьбы за информационную безопасность страны.		15
10	**Л 19–20.** Особенности прав собственности на информацию	2	
	СЗ 19–20. Решение задач на тему: «Криптографические методы защиты информации на персональном компьютере».	2	2
	ЛЗ 19–20. Решение кейсов на тему: «Криптографические методы защиты информации на персональном компьютере».	2	3

11	**СРОП 5.** Консультации по выполнению **СРО5**		
	Л 21-22. Системы информационной безопасности и защиты информации в организациях	2	
	СЗ 21–22. Решение задач на тему: «Криптографические методы защиты».	2	2
	ЛЗ 21–22. Решение кейсов на тему: «Криптографические методы защиты».	2	3
	СРО 5. Решение аналитического задания на тему: «Кибербезопасность»		20
МОДУЛЬ 4. ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ В КОМПЬЮТЕРАХ И КОМПЬЮТЕРНЫХ СЕТЯХ			
12	**Л23-24.** Программные средства защиты данных	2	
	СЗ 23–24. Решение задач на тему: «Требования к системам защиты информации автоматизированных систем от несанкционированного доступа».	2	2
	ЛЗ 23–24. Решение кейсов на тему: «Требования к системам защиты информации автоматизированных систем от несанкционированного доступа».	2	3
13	**СРСП 6.** Кейс-задание «Институты информации ограниченного доступа (тайны)		
	Л 25–26. Защита программного обеспечения от несанкционированного доступа	2	
	СЗ 25–26. Решение задач на тему: «Государственная, коммерческая, служебная, профессиональная тайна, персональные данные.	2	2
	ЛЗ 25–26. Решение кейсов на тему: «Государственная, коммерческая, служебная, профессиональная тайна, персональные данные.	2	3
14	**СРСП 6.** Консультации по выполнению **СРО6**		
	Л 27-28. Вирусы и антивирусные средства	2	
	СЗ 27–28. Решение задач на тему: «Методы защиты от вирусов»	2	2
	ЛЗ 27-ЛЗ 27. Решение кейсов на тему: «Методы защиты от вирусов»		3
15	**СРО 6** Эссе Кейс-задание «Как лечить вирусы?»		20
	Л 29–30. Защита в компьютерных сетях.	2	
	СЗ 29-СЗ 30. Решение задач на тему: «Угрозы безопасности информации и основные уязвимости информации»	2	5
	ЛЗ 29–30. Решение кейсов на тему: «Угрозы безопасности информации и основные уязвимости информации»		5
	СРОП 7. Консультация по подготовке к итоговому контролю		
Рубежный контроль 2			**100**
Итоговый контроль (экзамен)			**100**
ИТОГО за дисциплину			**100**

Декан _____ Байгунаков Д.С.

Председатель Академического комитета
по качеству преподавания и обучения _____ Бижанова М.Т.

Заведующий кафедрой _____ Мырзабекова Р.С.

Лектор _____ Жакишева С.А.
Ассистент _____ Холжабай М.А.

РУБРИКАТОР СУММАТИВНОГО ОЦЕНИВАНИЯ

КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Название задания СРО 1. Решение проектного задания «История шпионажа и мероприятий по защите информации и сохранению государственной и коммерческой тайны». (20% от 100% РК)

Критерий	**«Отлично»** **Макс. вес в %** 20–25%	**«Хорошо»** **Макс. вес в %** 15–20%	**«Удовлетворительно»** **Макс. вес в %** 10–15%	**«Неудовлетворительно»** **Макс. вес в % 0–10%**
Понимание и определение таких свойств информации как конфиденциальность; целостность, доступность.	Глубокое понимание и определение таких свойств информации как конфиденциальность; целостность, доступность.	Понимание и определение таких свойств информации как конфиденциальность; целостность, доступность.	Ограниченное понимание и определение таких свойств информации как конфиденциальность; целостность, доступность.	Поверхностное понимание и определение таких свойств информации как конфиденциальность; целостность, доступность.
Анализ основных форм шпионажа в условиях гибридных войн	Подробный анализ основных форм шпионажа в условиях гибридных войн	Анализ основных форм шпионажа в условиях гибридных войн	Удовлетворительный анализ основных форм шпионажа в условиях гибридных войн	Поверхностный анализ основных форм шпионажа в условиях гибридных войн
Анализ основных принципов информационной безопасности и защиты информации.	Глубокий анализ основных принципов информационной безопасности и защиты информации	Анализ основных принципов информационной безопасности и защиты информации	Ограниченный анализ основных принципов информационной безопасности и защиты информации	Поверхностный анализ основных принципов информационной безопасности и защиты информации
Проведение классификации носителей защищаемой информации	Всесторонняя классификация носителей защищаемой информации	Классификация носителей защищаемой информации	Ограниченная классификация носителей защищаемой информации	Поверхностная классификациия носителей защищаемой информации
Презентация, командная работа	Отличная, привлекательная презентация, отличное качество визуальных эффектов, слайдов, материалов, отличная командная работа.	Хорошая вовлеченность, хорошее качество визуальных эффектов, слайдов или других материалов, хороший уровень командной работы.	Удовлетворительный уровень вовлеченности, удовлетворительное качество материалов, удовлетворительный уровень командной работы.	Низкий уровень вовлеченности, низкое качество материалов, плохой уровень командной работы.

Название задания СРО 2. Решение аналитического задания на тему: «Понятие, сущность и цели защиты информации» (15% от 100% РК)

Критерий	**«Отлично»** **Макс. вес в %** 20–25%	**«Хорошо»** **Макс. вес в %** 15–20%	**«Удовлетворительно»** **Макс. вес в %** 10–15%	**«Неудовлетворительно»** **Макс. вес в % 0–10%**
Раскрытие понятий и сущности защиты информации как деятельности	Полное раскрытие понятий и сущности защиты информации как деятельности	Раскрытие понятий и сущности защиты информации как деятельности	Ограниченное раскрытие понятий и сущности защиты информации как деятельности	Поверхностное раскрытие понятий и сущности защиты информации как деятельности

Определение цели и задач защиты информации как деятельности	Отличное определение цели и задач защиты информации как деятельности	Определение цели и задач защиты информации как деятельности	Ограниченное определение цели и задач защиты информации как деятельности	Поверхностное определение цели и задач защиты информации как деятельности
Раскрытие различных видов защиты информации (правовая, техническая, криптографическая, физическая)	Конкретное раскрытие различных видов защиты информации (правовая, техническая, криптографическая, физическая)	Раскрытие различных видов защиты информации (правовая, техническая, криптографическая, физическая)	Удовлетворительное раскрытие различных видов защиты информации (правовая, техническая, криптографическая, физическая)	Ограниченное раскрытие различных видов защиты информации (правовая, техническая, криптографическая, физическая)
Презентация, индивидуальная/ командная работа	Отличная, привлекательная презентация, отличное качество визуальных эффектов, слайдов, материалов, отличная командная работа.	Хорошая вовлеченность, хорошее качество визуальных эффектов, слайдов или других материалов, хороший уровень командной работы.	Удовлетворительный уровень вовлеченности, удовлетворительное качество материалов, удовлетворительный уровень командной работы.	Низкий уровень вовлеченности, низкое качество материалов, плохой уровень командной работы.

Название задания СРО 3. Проектное задание на тему «Сетевая безопасность» (20% от 100% РК).

Критерий	**«Отлично»** **Макс. вес в %** 20–25%	**«Хорошо»** **Макс. вес в %** 15–20%	**«Удовлетворительно»** **Макс. вес в %** 10–15%	**«Неудовлетворительно»** **Макс. вес в % 0–10%**
Описание угроз сетевой безопасности	Подробное описание угроз сетевой безопасности	Описание угроз сетевой безопасности	Ограниченное описание угроз сетевой безопасности	Поверхностное описание угроз сетевой безопасности
Раскрытие сущности защиты информации как деятельности	Полное раскрытие и оценка современного состояния электронных архивов в РК и за рубежом, преимуществ электронного архива.	Раскрытие и оценка современного состояния электронных архивов в РК и за рубежом, преимуществ электронного архива.	Ограниченное раскрытие и оценка современного состояния электронных архивов в РК и за рубежом, преимуществ электронного архива.	Незначительное раскрытие и оценка современного состояния электронных архивов в РК и за рубежом, преимуществ электронного архива.
Анализ типов сетевых атак	Глубокий анализ типов сетевых атак	Анализ типов сетевых атак	Ограниченный анализ типов сетевых атак	Поверхностный анализ типов сетевых атак
Оценка видов защиты сети	Разносторонняя оценка видов защиты сети	Оценка видов защиты сети	Ограничесннная оценка видов защиты сети	Поверхностная оценка видов защиты сети
Раскрытие методов сетевой защиты	Полное раскрытие методов сетевой защиты	Раскрытие методов сетевой защиты	Неполное раскрытие методов сетевой защиты	Поверхностное раскрытие методов сетевой защиты
Презентация, индивидуальная/командная работа	Отличная, привлекательная презентация, отличное качество визуальных эффектов, слайдов, материалов, отличная командная работа.	Хорошая вовлеченность, хорошее качество визуальных эффектов, слайдов или других материалов, хороший уровень командной работы.	Удовлетворительный уровень вовлеченности, удовлетворительное качество материалов, удовлетворительный уровень командной работы.	Низкий уровень вовлеченности, низкое качество материалов, плохой уровень командной работы.

Название задания СРО 4. Решение проектного задания «Информационная война в системе международных отношений» (15% от 100% РК)

Критерий	«Отлично» **Макс. вес в %** 20–25%	«Хорошо» **Макс. вес в %** 15–20%	«Удовлетворительно» **Макс. вес в %** 10–15%	«Неудовлетворительно» **Макс. вес в % 0–10%**
Рассмотрение сущности, основных черт и методов информационных войн	Полное рассмотрение сущности, основных черт и методов информационных войн	Рассмотрение сущности, основных черт и методов информационных войн	Ограниченное рассмотрение сущности, основных черт и методов информационных войн	Поверхностное рассмотрение сущности, основных черт и методов информационных войн
Осведомленность о путях воздействия на сознание людей в условиях информационной войны	Глубокая осведомленность о путях воздействия на сознание людей в условиях информационной войны	Осведомленность о путях воздействия на сознание людей в условиях информационной войны	Ограниченная осведомленность о путях воздействия на сознание людей в условиях информационной войны	Незначительная осведомленность о путях воздействия на сознание людей в условиях информационной войны
Анализ методов борьбы за информационную безопасность страны	Глубокий анализ методов борьбы за информационную безопасность страны	Анализ методов борьбы за информационную безопасность страны	Ограниченный анализ методов борьбы за информационную безопасность страны	Поверхностный анализ методов борьбы за информационную безопасность страны
Подготовка и защита реферативной работы по проблеме	Отличная подготовка и защита реферативной работы по проблеме.	Хорошая подготовка и защита реферативной работы по проблеме	Удовлетворительная подготовка и защита реферативной работы по проблеме	Плохая подготовка и защита реферативной работы по проблеме

Название задания СРО 5. Решение проектного задания «Кибербезопасность» (20 % от 100% РК).

Критерий	«Отлично» **Макс. вес в %** 20–25%	«Хорошо» **Макс. вес в %** 15–20%	«Удовлетворительно» **Макс. вес в %** 10–15%	«Неудовлетворительно» **Макс. вес в % 0–10%**
Обоснование потребности в кибербезопасности	Обоснованное мнение о потребности в кибербезопасности	Обоснование потребности в кибербезопасности	Ограниченный Обоснование потребности в кибербезопасности	Поверхностный Обоснование потребности в кибербезопасности
Описание угрозы кибербезопасности, сущности, целей и задач защиты информации как деятельности	Глубокая осведомленность о рейтинговых международных проектах сохранения культурного (архивного) наследия в цифровом формате.	Описание угрозы кибербезопасности, сущности, целей и задач защиты информации как деятельности	Ограниченное описание угрозы кибербезопасности, сущности, целей и задач защиты информации как деятельности	Непонимание угрозы кибербезопасности, сущности, целей и задач защиты информации как деятельности
Оценка юридических и этических проблем кибербезопасности	Четкая и глубокая оценка юридических и этических проблем кибербезопасности	Оценка юридических и этических проблем кибербезопасности	Ограниченная оценка юридических и этических проблем кибербезопасности	Неудовлетворительная оценка юридических и этических проблем кибербезопасности
Оценка профиля киберпреступников	Глубокая оценка профиля киберпреступников	Оценка профиля киберпреступников	Ограниченная оценка профиля киберпреступников	Неудовлетворительная оценка профиля киберпреступников
Раскрытие понятия кибервойны, конфликтов в киберпространстве	Глубокое раскрытие понятия кибервойны, конфликтов в киберпространстве	Раскрытие понятия кибервойны, конфликтов в киберпространстве	Ограниченное раскрытие понятия кибервойны, конфликтов в киберпространстве	Неудовлетворительное раскрытие понятия кибервойны, конфликтов в киберпространстве

Название задания СРО 6. Решение Кейс-задания и Эссе «Как лечить вирусы?» (20% от 100% РК).

Критерий	«Отлично» **Макс. вес в %** 20–25%	«Хорошо» **Макс. вес в %** 15–20%	«Удовлетворительно» **Макс. вес в %** 10–15%	«Неудовлетворительно» **Макс. вес в % 0–10%**
Понимание природы компьютерных вирусов	Глубинное понимание природы компьютерных вирусов	Понимание природы компьютерных вирусов	Ограниченное понимание природы компьютерных вирусов	Поверхностное понимание природы компьютерных вирусов
Осведомленность о способах лечения компьютерных вирусов	Полная осведомленность о способах лечения компьютерных вирусов	Осведомленность о способах лечения компьютерных вирусов	Ограниченная осведомленность о способах лечения компьютерных вирусов	Незначительная осведомленность о способах лечения компьютерных вирусов
Использование инструментальных средств, доступных пользователям сети для защиты устройств от атак и помощи в удалении вредоносного программного обеспечения из зараженных компьютеров.	Широкое использование инструментальных средств, доступных пользователям сети для защиты устройств от атак и помощи в удалении вредоносного программного обеспечения из зараженных компьютеров.	Использование инструментальных средств, доступных пользователям сети для защиты устройств от атак и помощи в удалении вредоносного программного обеспечения из зараженных компьютеров.	Ограниченное использование инструментальных средств, доступных пользователям сети для защиты устройств от атак и помощи в удалении вредоносного программного обеспечения из зараженных компьютеров.	Нет представления об использовании инструментальных средств, доступных пользователям сети для защиты устройств от атак и помощи в удалении вредоносного программного обеспечения из зараженных компьютеров.
Подготовка и защита эссе	Отличная подготовка и защита эссе по проблеме.	Хорошая подготовка и защита эссе по проблеме	Удовлетворительная подготовка и защита эссе по проблеме	Плохая подготовка и защита эссе по проблеме