Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Институт информационных технологий и анализа данных»

УТВЕРЖДЕНА:
на заседании Совета института ИТиАД им. Е.И.Попова
Протокол №8 от 24 февраля 2025 г.

Рабочая программа дисциплины

«КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление: 10.04.01 Информационная безопасность

Безопасность киберфизических систем

Квалификация: Магистр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Маринов Александр Андреевич Дата подписания: 22.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 23.06.2025	Документ подписан простой электронной подписью Согласовал: Маринов Александр Андреевич Дата подписания: 22.06.2025

Год набора – 2025

Иркутск, 2025 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Комплексное обеспечение информационной безопасности» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ПК-6 Способность разрабатывать технические задания на проектирование систем обеспечения информационной безопасности или информационно-аналитических систем безопасности	ПК-6.1

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПК-6.1	Разрабатывает системы, комплексы, средства и технологии обеспечения информационной безопасности, а также программы и методики испытаний средств и систем обеспечения информационной безопасности	**Знать** средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации. **Уметь** пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения. **Владеть** методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Комплексное обеспечение информационной безопасности» базируется на результатах освоения следующих дисциплин/практик: «Организационно-правовые механизмы обеспечения информационной безопасности», «Управление информационной безопасностью», «Технологии обеспечения информационной безопасности объектов»

Дисциплина является предшествующей для дисциплин/практик: «Организационно-правовые механизмы обеспечения информационной безопасности»

3 Объем дисциплины

Объем дисциплины составляет – 5 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 2
Общая трудоемкость дисциплины	180	180
Аудиторные занятия, в том числе:	104	104
лекции	52	52
лабораторные работы	0	0
практические/семинарские занятия	52	52
Самостоятельная работа (в т.ч. курсовое проектирование)	40	40
Трудоемкость промежуточной аттестации	36	36
Вид промежуточной аттестации (итогового контроля по дисциплине)	Экзамен	Экзамен

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 2

№ п/п	**Наименование раздела и темы дисциплины**	**Виды контактной работы**						СРС		**Форма текущего контроля**
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Введение в комплексное обеспечение информационной безопасности	1	8			1	8	1	6	Устный опрос
2	Классификация методов защиты информации для предприятий и организаций	2	8			2	8	1	4	Устный опрос
3	Организационно-правовые методы в системе компьютерной безопасности	3	8			3	8	1	6	Устный опрос
4	Физические методы защиты информации при хранении на компьютерах и передаче по сетям	4	7			4	7	1	4	Устный опрос
5	Технические методы защиты в экономике и бизнесе	5	7			5	7	1	6	Устный опрос

6	Математические проблемы построения модели безопасности комплексных систем защиты данных	6	7			6	7	1	6	Устный опрос
7	Обзор криптографических методов защиты информации в экономике и бизнесе. Построение комплексной системы защиты информации на предприятии	7	7			7	7	1	8	Устный опрос
	Промежуточная аттестация								36	Экзамен
	Всего		52				52		76	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 2

№	Тема	Краткое содержание
1	Введение в комплексное обеспечение информационной безопасности	Значение экономической и банковской информации в жизни современного общества. Проблемы защиты информации. Типы нарушений. Характеристика современных видов атак на банковские структуры и системы. Общая характеристика задач комплексной защиты информационной безопасности. Угрозы информационной безопасности и их классификация.
2	Классификация методов защиты информации для предприятий и организаций	Обзор методов и средств защиты банковской и экономической информации. Комплексный подход как современная парадигма решения задач в сфере безопасности экономической информации. Физические, организационно-правовые и технические методы, особенности их применения в сфере безопасности экономической информации.
3	Организационно-правовые методы в системе компьютерной безопасности	Основные законы и постановления правительства РФ в сфере решения задач защиты информации в экономических системах. Основные положения федеральных законов "Об электронной подписи" 2011 года, законы "О персональных данных", "О коммерческой информации". Современные проблемы в сфере хранения и передаче конфиденциальной экономической информации.
4	Физические методы	Развертывание системы физической защиты

	защиты информации при хранении на компьютерах и передаче по сетям	информации на предприятии. Допуск сотрудников к к работе с конфиденциальной информацией. Технические средства ограничения и предупреждения несанкционированного допуска к экономической информации. Роль физических методов защиты информации в общей структуре комплексной защиты данных.
5	Технические методы защиты в экономике и бизнесе	Разворачивание системы комплексной защиты информации на предприятии, оценка информационных активов, анализ рисков и выбор адекватной системы защиты данных и содержащей ее инфраструктуры. Технические средства защиты информации. Использование стандартов информационной безопасности. Серия Европейских стандартов 27000.
6	Математические проблемы построения модели безопасности комплексных систем защиты данных	Введение в проблематику математических проблем, связанных с защитой данных. Математические основы построения электронных цифровых подписей, проверка подлинности информации. Методы аутентификации и поддержки конфиденциальности в сфере экономики. Модели систем комплексного обеспечения информационной безопасности.
7	Обзор криптографических методов защиты информации в экономике и бизнесе. Построение комплексной системы защиты информации на предприятии	Криптографические методы и средства защиты информации: классические методы шифрования, хеш-функции, методы шифрования с открытым ключом. Решение проблемы распространения ключей, удаленная аутентификация пользователей. Технология 3D-Secure - современная парадигма в электронной коммерции. Разграничение зон ответственности сторон в электронной коммерции.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 2

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Введение в комплексное обеспечение информационной безопасности	8
2	Классификация методов защиты информации для предприятий и организаций	8
3	Организационно-правовые методы в системе компьютерной безопасности	8
4	Физические методы защиты информации при хранении на компьютерах и передаче по сетям	7

5	Технические методы защиты в экономике и бизнесе	7
6	Математические проблемы построения модели безопасности комплексных систем защиты данных	7
7	Обзор криптографических методов защиты информации в экономике и бизнесе. Построение комплексной системы защиты информации на предприятии	7

4.5 Самостоятельная работа

Семестр № 2

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	40

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: брейн-ринг; банк вопросов; интеллектуальный биатлон

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

https://el.istu.edu/mod/folder/view.php?id=335348

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/mod/folder/view.php?id=335350

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 2 | Устный опрос

Описание процедуры.

Проведение устного опроса в форме «вопрос-ответ»

Критерии оценивания.

ответ раскрыт полностью 8-10 баллов
ответ раскрыт частично 4-7 баллов
имеет только общее представление о проблеме 2-4 баллов
не ответил – 0 баллов

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	Критерии оценивания	Средства (методы) оценивания промежуточной аттестации
ПК-6.1	Знает средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации.	Устное собеседование по теоретическим вопросам.

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 2, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

Устный экзамен по дисциплине проводится в соответствии с государственными общеобразовательными стандартами. Экзамен проводится и использованием комплекта билетов. Количество билетов должно превышать количество учащихся в группе. Экзаменационные билеты должны содержать два теоретических вопроса и задачу. Расположив на столе экзаменационные билеты в произвольном порядке, преподаватель приглашает к столу учащегося. Выбрав билет, учащийся называет вслух его номер. Преподаватель записывает номер билета в экзаменационную ведомость и выдает учащемуся проштампованный лист для подготовки ответа. Одновременно в аудитории готовится к ответу должны не более 5 человек. Время подготовки к ответу, в зависимости от сложности предмета 20-40 мин. Учащиеся приступают в работе над ответами на билеты. Задача преподавателя на этом этапе контролировать ситуацию. Учащиеся, нарушающие дисциплину (устраивающие переговоры, списывающие и т.д.) лишаются права сдавать экзамен.

Пример задания:

1. Сформулируйте определение электронной цифровой подписи.
2. Какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз?
3. Экономическая информация как товар и объект безопасности.
4. Принципы построения и функционирования межсетевых экранов.
5. Классификация межсетевых экранов.
6. ЭП на основе симметричных криптоалгоритмов. ЭП на основе асимметричных криптоалгоритмов.

7. Алгоритм хеширования SHA-2.
8. Протоколы VPN. Протоколы канального, сетевого и сеансового уровней.
9. Общая характеристика СБД АС.
10. Государственное регулирование информационной безопасности в РФ.
11. Доктрина информационной безопасности России.
12. Модели систем комплексного обеспечения информационной безопасности.
13. Фрагментарный и системный подход к защите информации.
14. Методы и средства защиты информации.
15. Федеральные законы в сфере информатизации и информационной безопасности в РФ.
16. Уголовно-правовой контроль над компьютерной преступностью в РФ.
17. Политика безопасности и ее принципы.
18. Методы аутентификации и поддержки конфиденциальности в сфере экономики.
19. Задачи ИБ в программе « цифровая экономика»
20. Организационное обеспечение ИБ.
21. Организация конфиденциального делопроизводства.

6.2.2.1.2 Критерии оценивания

Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
На высоком уровне демонстрирует знание основных методик защиты информации и их практическое применение; владение навыками обеспечения информационной безопасности; знание классификации угроз информационной безопасности; умение использовать специализированное программное обеспечение для информационной защиты; владение навыками осуществлять организацию информационной защиты, охраны	С незначительными неточностями демонстрирует знание основных методик защиты информации и их практическое применение; умение определять возможные источники угроз информационной безопасности; владение навыками обеспечения информационной и экономической безопасности; знание классификации угроз информационной безопасности; умение использовать специализированное программное обеспечение для	Частично демонстрирует знание основных методик защиты информации и их практическое применение; умение определять возможные источники угроз информационной и экономической безопасности хозяйствующих субъектов; владение навыками обеспечения информационной и экономической безопасности; знание классификации угроз экономической и информационной безопасности; умение использовать специализированное программное обеспечение для	Демонстрирует отсутствие знания основных методик защиты информации и их практическое применение; умение определять возможные источники угроз информационной безопасности хозяйствующих субъектов; владение навыками обеспечения информационной и экономической безопасности; знание классификации угроз экономической и информационной безопасности; умение использовать специализированное программное обеспечение для информационной защиты; владение навыками осуществлять организацию

интеллектуальной собственности с использованием технических и программных средств.	информационной защиты.	информационной защиты; владение навыками осуществлять организацию информационной защиты, охраны интеллектуальной собственности с использованием технических и программных средств.	информационной защиты, охраны интеллектуальной собственности с использованием технических и программных средств.

7 Основная учебная литература

1. Мельников В. П. Информационная безопасность и защита информации : учебное пособие для вузов по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова, 2011. - 330.

8 Дополнительная учебная литература и справочная

1. Мельников В. П. Информационная безопасность и защита информации : учебное пособие для студентов высшего профессионального образования ; под ред. С. А. Клейменова / В. П. Мельников, С. А. Клейменов, А. М. Петраков, 2011. - 336.

2. Партыка Т. Л. Вычислительная техника : учеб. пособие для сред. проф. образования по группе специальностей "Электротехника" / Т. Л. Партыка, И. И. Попов, 2007. - 607.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional (Microsoft Windows Seven Starter) - Seven, Vista, XP_prof_64, XP_prof_32 - поставка 2010

2. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional [1x100] RUS (проведен апгрейд с Microsoft Windows Seven Starter [1x100]) - поставка 2010

3. Свободно распространяемое программное обеспечение Microsoft Windows Server Standard 2008 R2 Russian Academic OPEN 1 License No Level

12 Материально-техническое обеспечение дисциплины

1. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

2. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

3. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

4. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

5. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

6. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

7. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

8. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

9. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

10. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

11. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

12. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

13. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

14. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

15. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

16. МФУ FS-1128 MFP

17. Проектор Epson EB-W04LCD.WXGA 1280*800.3000:1.2800 ANSI Lumens

18. Сервер CPU Intel Core i7-960/GA-X58A-UD3R/DDR-IIIDimm 2Gb/HDD 1 Tb/DVD-RW/512MB PCI-E/блок пит.+ПО