

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
(121)»

УТВЕРЖДЕНА:
на заседании совета института ИТиАД им. Е.И.Попова
Протокол №8 от 16 февраля 2026 г.

Рабочая программа дисциплины

«ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ»

Направление: 10.03.01 Информационная безопасность

Организация и технологии защиты информации (в сфере техники и технологии)

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой
электронной подписью
Составитель программы:
Маринов Александр
Андреевич
Дата подписания: 18.06.2026

Документ подписан простой
электронной подписью
Утвердил: Говорков Алексей
Сергеевич
Дата подписания: 18.06.2026

Документ подписан простой
электронной подписью
Согласовал: Маринов
Александр Андреевич
Дата подписания: 18.06.2026

Год набора – 2026

Иркутск, 2026 г.

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

1.1 Дисциплина «Экономика защиты информации» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК ОС-11 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ОПК ОС-11.2
ОПК ОС-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	ОПК ОС-2.1.1

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-11.2	Способен принимать решение на основе экономического анализа, проводит изучение основных факторов под влиянием которых происходит развитие анализируемых систем, закономерностей их поведения, динамики изменения, а также, использование универсальной оценки защиты экономической информации	Знать современные подходы к экономическому анализу, структуру функционального анализа и основные классификации рисков. Уметь анализировать экономические показатели эффективности процессов, выявлять и структурировать риски, определять стоимость информации. Владеть навыками определения экономической эффективности механизмов обеспечения информационной безопасности.
ОПК ОС-2.1.1	Способен проводить анализ усложнённых экономических связей, принимать обоснованные решения защищённости объекта информатизации, а также проводить анализ оценки максимального правдоподобия (асимптотической теории вывода о значениях параметра ЗИ)	Знать подходы к определению экономических связей между процессами в системах, обеспечивающих информационную безопасность. Уметь рассчитывать влияние процессов обеспечения информационной безопасности и их отдельных составляющих на экономические показатели системы. Владеть методами экономического анализа, методами выбора показателей для оценки эффективности.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Экономика защиты информации» базируется на результатах освоения следующих дисциплин/практик: «Программирование в MathCad и MatLab»

Дисциплина является предшествующей для дисциплин/практик: «Основы проектной деятельности», «Основы управления информационной безопасностью», «Комплексная система защиты информации на предприятии»

3 Объем дисциплины

Объем дисциплины составляет – 4 ЗЕТ

Вид учебной работы	Трудоемкость в академических часах (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 3
Общая трудоемкость дисциплины	144	144
Аудиторные занятия, в том числе:	48	48
лекции	16	16
лабораторные работы	0	0
практические/семинарские занятия	32	32
Самостоятельная работа (в т.ч. курсовое проектирование)	60	60
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 № 3

№ 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	Методы анализа исходных данных для проектирования систем информационной безопасности	1	2			1	4	1	6	Устный опрос
2	Технико- экономическое обоснование проектов по обеспечению информационной безопасности	2	2			2	4	1	6	Устный опрос

3	Анализ функциональных процессов в системах защиты информации	3	2			3	3	1	6	Устный опрос
4	Идентификация источников информационных угроз в организациях	4	2			4	3	1	6	Устный опрос
5	Оценка ущерба от информационных атак	5	2			5	3	1	6	Устный опрос
6	Моделирование угроз в информационных системах	6	2			6	3	1	6	Устный опрос
7	Роль анализа данных в управлении рисками информационной безопасности	7	1			7	3	1	6	Устный опрос
8	Применение машинного обучения для анализа угроз информационной безопасности	8	1			8	3	1	6	Устный опрос
9	Сравнительный анализ существующих средств обеспечения информационной безопасности	9	1			9	3	1	6	Устный опрос
10	Кейс-стадии: успешные практики анализа угроз в организациях	10	1			10	3	1	6	Устный опрос
	Промежуточная аттестация								36	Экзамен
	Всего		16				32		96	

4.2 Краткое содержание разделов и тем занятий

Семестр № 3

№	Тема	Краткое содержание
1	Методы анализа исходных данных для проектирования систем информационной безопасности	Обзор существующих подходов и инструментов, используемых для анализа данных.
2	Технико-экономическое обоснование проектов по обеспечению информационной	Как провести ТЭО на примере конкретного проекта

	безопасности	
3	Анализ функциональных процессов в системах защиты информации	Методики выявления уязвимостей и угроз в бизнес-процессах
4	Идентификация источников информационных угроз в организациях	Классификация угроз и методов их выявления
5	Оценка ущерба от информационных атак	Подходы к количественной и качественной оценке потенциального ущерба для бизнеса
6	Моделирование угроз в информационных системах	Использование методов моделирования для анализа возможных сценариев атак.
7	Роль анализа данных в управлении рисками информационной безопасности	Как данные помогают в принятии решений по управлению рисками
8	Применение машинного обучения для анализа угроз информационной безопасности	Исследование применения алгоритмов машинного обучения для выявления аномалий и угроз.
9	Сравнительный анализ существующих средств обеспечения информационной безопасности	Оценка эффективности различных решений на основе анализа данных
10	Кейс-стадии: успешные практики анализа угроз в организациях	Изучение реальных примеров из практики, где анализ данных помог предотвратить или минимизировать последствия информационных атак.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 3

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Методы анализа исходных данных для проектирования систем информационной безопасности	4
2	Технико-экономическое обоснование проектов по обеспечению информационной безопасности	4
3	Анализ функциональных процессов в системах защиты информации	3
4	Идентификация источников информационных	3

	угроз в организациях	
5	Оценка ущерба от информационных атак	3
6	Моделирование угроз в информационных системах	3
7	Роль анализа данных в управлении рисками информационной безопасности	3
8	Применение машинного обучения для анализа угроз информационной безопасности	3
9	Сравнительный анализ существующих средств обеспечения информационной безопасности	3
10	Кейс-стадии: успешные практики анализа угроз в организациях	3

4.5 Самостоятельная работа

Семестр № 3

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	60

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: работа в группе

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/>

5.1.2 Методические указания для обучающихся по самостоятельной работе:

<https://el.istu.edu/>

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 3 | Устный опрос

Описание процедуры.

Устный опрос проводится по окончании лекционных занятий путем опроса студентов по списочному составу (при наличии бюджета времени после обсуждения установленных вопросов).

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
ОПК ОС-11.2	1. Умение идентифицировать и анализировать факторы, влияющие на развитие систем. 2. Способность выявлять закономерности и тренды в поведении систем. 3. Умение принимать решения на основе проведенного экономического анализа. 4. Способность применять универсальные методы оценки защиты экономической информации.	Устное собеседование по теоретическим вопросам. Тест.
ОПК ОС-2.1.1	1. Способность выявлять и анализировать сложные экономические связи в заданной системе. 2. Умение принимать обоснованные решения по обеспечению защищенности объектов информатизации. 3. Способность использовать методы максимального правдоподобия для оценки параметров. 4. Умение четко и логично представлять результаты анализа	Устное собеседование по теоретическим вопросам. Тест.

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 3, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

- 1) Экзамен по дисциплине проводится согласно расписанию в назначенной аудитории, в которую приглашается к установленному началу экзамена группа студентов.
- 2) К экзамену допускаются студенты, которые выполнили все предусмотренные работы по освоению курса: сданы практические работы по выбранной теме.
- 3) Каждый студент из числа допущенных выбирает один билет и готовится к

ответу в течение не менее 30 - 45 минут письменно на поставленные два вопроса в билете.

6.2.2.1.2 Критерии оценивания

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Уверенно и без ошибок отвечает на все вопросы билета	Допускает незначительные ошибки в ответе на один из вопросов, включая дополнительные по результатам собеседования	Знает ответы на два вопроса или допускает ошибки в ответах на вопросы	Не отвечает на два и более вопросов

7 Основная учебная литература

1. Прокофьев И.В. Защита информации в информационных интегрированных системах : учеб. для вузов по специальности "Управление качеством" / И.В. Прокофьев, 2002. - 137.

2. Попова Е. С. Информационная безопасность и защита информации [Электронный ресурс] : курс лекций / Е. С. Попова, 2009. - 68.

[Сайт] – URL: <http://elib.istu.edu/viewer/view.php?file=/files/er-4183.pdf>

3. Шепитько Г. Е. Экономика защиты информации : учебное пособие / Г. Е. Шепитько, 2011. - 64.

8 Дополнительная учебная литература и справочная

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, 2009. - 330.

2. 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.

3. Северин В. А. Правовая защита информации в коммерческих организациях : учебное пособие для вузов по специальности "Юриспруденция" направления "Юриспруденция" / В. А. Северин; под ред. Б. И. Пугинского, 2009. - 219.

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