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

«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

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: 22.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 23.06.2025	Документ подписан простой электронной подписью Согласовал: Сибиряк Юрий Владимирович Дата подписания: 23.06.2025

Год набора – 2025

Иркутск, 2025 г.

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

1.1 Дисциплина «Основы управления информационной безопасностью» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК ОС-10 Способность проводить эксперименты по моделированию технологических процессов используя языки программирования и технологии разработки программных средств для обработки информации в специальных АИС с заданной степенью статистической надежности результатов и учетом оценки их погрешности и достоверности	ОПК ОС-10.2
ОПК ОС-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК ОС-2.3.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-10.2	Использует выбранную среду объекта информатизации для экспериментов по моделированию технологических процессов обработки информации в специальных АИС; способен разработать процедуру интеграции модулей защиты в бизнес-процессы (включая международную практику)	**Знать** информационную среду объектов информатизации для экспериментов по моделированию технологических процессов обработки информации в специальных АИС. **Уметь** применять с целью защиты информации технические, программные и программно-технические средства в вопросах систем менеджмента информационной безопасности. **Владеть** некриптографическими методами безопасности данных, подлежащих защите в соответствии с действующим законодательством. Показать на практике процесс интеграции модулей защиты в бизнес-процессы (включая международную практику).
ОПК ОС-2.3.2	Способен проводить эксперименты по моделированию технологических процессов обработки информации в специальных АИС с заданной	**Знать** основные методы и подходы к моделированию технологических процессов в специальных АИС; статистические методы оценки надежности и точности моделей; основные параметры, влияющие на

	степенью статистической надежности результатов; знает способы и методы реализации несанкционированного доступа к информации и специальные программные воздействия на информацию и ее носители в автоматизированных системах	результаты моделирования; методы и инструменты, используемые для несанкционированного доступа к данным; методы обнаружения несанкционированного доступа. **Уметь** проводить эксперименты с использованием различных методов моделирования технологических процессов в специальных АИС; анализировать и интерпретировать результаты экспериментов; оценивать статистическую надежность полученных результатов. **Владеть** методами проектирования и проведение экспериментов по моделированию технологических процессов обработки информации в специальных АИС.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Основы управления информационной безопасностью» базируется на результатах освоения следующих дисциплин/практик: «Сети и системы передачи информации», «Организационное и правовое обеспечение информационной безопасности», «Теория принятия решений», «Программно-аппаратные средства защиты информации», «Техническая защита информации», «Аудит информационной безопасности», «Экономика защиты информации»

Дисциплина является предшествующей для дисциплин/практик: «Производственная практика: преддипломная практика»

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 № 8
Общая трудоемкость дисциплины	144	144
Аудиторные занятия, в том числе:	48	48
лекции	32	32
лабораторные работы	0	0
практические/семинарские занятия	16	16
Самостоятельная работа (в т.ч. курсовое проектирование)	96	96
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет с оценкой	Зачет с оценкой

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 8

№ 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	Моделирование технологических процессов обработки информации в специальной АИС	1	4			1	2	1	10	Устный опрос
2	Интеграция модулей защиты в бизнес-процессы: международные практики и стандарты	2	4			2	2	1	10	Устный опрос
3	Статистическая надежность результатов экспериментов в моделировании АИС	3	3			3	1	1	9	Устный опрос
4	Методы несанкционированного доступа: анализ и предотвращение	4	3			4	2	1	10	Устный опрос
5	Программное обеспечение для тестирования безопасности АИС	5	3			5	1	1	9	Устный опрос
6	Разработка процедур защиты информации в автоматизированных системах	6	3			6	2	1	10	Устный опрос
7	Кейс-стадии успешных интеграций модулей защиты в бизнес-процессы	7	3			7	1	1	9	Устный опрос
8	Моделирование сценариев атак на АИС и их последствия	8	3			8	2	1	10	Устный опрос
9	Этические аспекты и правовые нормы в области несанкционированного доступа к информации	9	3			9	1	1	9	Устный опрос
10	Методы	10	3			10	2	1	10	Устный

	повышения устойчивости АИС к специальным программным воздействиям									опрос
	Промежуточная аттестация									Зачет с оценкой
	Всего		32				16		96	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 8

№	Тема	Краткое содержание
1	Моделирование технологических процессов обработки информации в специальной АИС	Разработка и анализ моделей, описывающих процессы в различных автоматизированных системах.
2	Интеграция модулей защиты в бизнес-процессы: международные практики и стандарты	Исследование подходов к интеграции систем безопасности в бизнес-процессы с акцентом на международные стандарты (например, ISO 27001).
3	Статистическая надежность результатов экспериментов в моделировании АИС	Методы оценки и повышения статистической надежности результатов при проведении экспериментов.
4	Методы несанкционированного доступа: анализ и предотвращение	Изучение способов, используемых для взлома информационных систем, и разработка методов защиты от них.
5	Программное обеспечение для тестирования безопасности АИС	Обзор инструментов и технологий для моделирования атак и оценки уязвимостей систем.
6	Разработка процедур защиты информации в автоматизированных системах	Создание протоколов и рекомендаций по защите данных в контексте бизнес-процессов.
7	Кейс-стадии успешных интеграций модулей защиты в бизнес-процессы	Анализ реальных примеров успешной интеграции систем безопасности и их влияние на эффективность бизнеса.
8	Моделирование сценариев атак на АИС и их последствия	Создание и анализ сценариев возможных атак для оценки устойчивости систем.
9	Этические аспекты и правовые нормы в области несанкционированного доступа к информации	Обсуждение правовых последствий и этических норм, связанных с информационной безопасностью.

10	Методы повышения устойчивости АИС к специальным программным воздействиям	Исследование технологий и подходов, направленных на защиту информации от вредоносных программ и атак: Тестирование и оценка надёжности. Регулярное и систематическое тестирование позволяет выявлять и устранять проблемы на ранних стадиях разработки; Управление рисками. Идентификация, анализ и оценка потенциальных угроз помогают организациям принимать обоснованные решения о мерах по обеспечению надёжности; Принцип «безопасность по умолчанию». Система должна быть построена с максимальной степенью безопасности изначально. Интеграция безопасности во все аспекты разработки, начиная с архитектуры и заканчивая кодированием; Использование DevOps-методологий. Они интегрируют процессы разработки и эксплуатации, обеспечивая непрерывность и автоматизацию. Это способствует более быстрой реакции на изменения и устранение дефектов; Применение средств обеспечения безопасности. Программы антивирусной защиты и системы обнаружения вторжений обеспечивают высокий уровень защиты от внешних и внутренних угроз; Использование искусственного интеллекта и машинного обучения. Алгоритмы машинного обучения и искусственного интеллекта применяются для анализа данных, выявления аномалий и предсказания возможных проблем; Принципы безопасного программирования. Правильное управление аутентификацией и авторизацией, санитарное программирование, шифрование данных и другие практики направлены на предотвращение уязвимостей и атак.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 8

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Моделирование технологических процессов обработки данных в АИС	2
2	Интеграция модулей защиты в бизнес-процессы: международные практики и стандарты	2
3	Статистическая надежность результатов	1

	экспериментов в моделировании АИС	
4	Методы несанкционированного доступа: анализ и предотвращение	2
5	Программное обеспечение для тестирования безопасности АИС	1
6	Разработка процедур защиты информации в автоматизированных системах	2
7	Кейс-стадии успешных интеграций модулей защиты в бизнес-процессы	1
8	Моделирование сценариев атак на АИС и их последствия	2
9	Этические аспекты и правовые нормы в области несанкционированного доступа к информации	1
10	Методы повышения устойчивости АИС к специальным программным воздействиям	2

4.5 Самостоятельная работа

Семестр № 8

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	96

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: интерактивная демонстрация способа решения типовой проблемы, работа в парах

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/course/index.php?categoryid=1198

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/course/index.php?categoryid=1198

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 8 | Устный опрос

Описание процедуры.

Устный опрос проводится по окончанию лекционных занятий путем опроса студентов по списочному составу (при наличии бюджета времени после обсуждения установленных вопросов).
Пример задания:
представлены в настоящей РПД по соответствующим темам (таблица раздела 4.2

«Краткое содержание разделов и тем занятий»).

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-10.2	Способен продемонстрировать специализированные знания в области защиты информации	Способен продемонстрировать знания способов и методов реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах, а также навыки проведения экспериментов по моделированию технологических процессов обработки информации в специальных АИС.
ОПК ОС-2.3.2	Способен продемонстрировать знания способов и методов реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в	Устное собеседование по теоретическим вопросам и/или выполнение практически

	автоматизированных системах, а также навыки проведения экспериментов по моделированию технологических процессов обработки информации в специальных АИС	заданий

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 8, Типовые оценочные средства для проведения дифференцированного зачета по дисциплине

6.2.2.1.1 Описание процедуры

1)Дифференцированный зачет по дисциплине проводится согласно расписанию в назначенной
аудитории, в которую приглашается к установленному началу ,зачета группа студентов.
2) К дифференцированному зачету 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 три вопроса в билете.
1. Какие основные этапы включает в себя процесс моделирования технологических процессов в АИС?
2. Каковы основные методы моделирования, используемые для описания процессов обработки информации?
3. Какие факторы необходимо учитывать при разработке модели для автоматизированной системы?
4. Приведите примеры применения моделирования в реальных автоматизированных системах.
5. Какие международные стандарты существуют для интеграции систем безопасности в бизнес-процессы?
6. Каковы основные этапы интеграции модулей защиты в существующие бизнес-процессы?
7. Приведите примеры успешной интеграции модулей защиты в бизнес-процессы.
8. Каковы основные методы оценки статистической надежности результатов экспериментов?
9. Какие факторы могут влиять на статистическую надежность моделей в АИС?
10. Как можно повысить надежность результатов при проведении экспериментов в моделировании?
11. Какие существуют основные методы несанкционированного доступа к информационным системам?
12. Каковы признаки того, что система подверглась несанкционированному доступу?
13. Какие меры можно предпринять для предотвращения несанкционированного доступа к АИС?
14. Какие инструменты наиболее распространены для тестирования безопасности автоматизированных систем?
15. Каковы основные этапы проведения тестирования безопасности АИС с использованием программного обеспечения?
16. В чем заключается разница между статическим и динамическим тестированием безопасности?
17. Как можно оценить эффективность программного обеспечения для тестирования

безопасности?
18. Какие ключевые элементы должны быть включены в процедуры защиты информации в АИС?
19. Каковы основные подходы к разработке эффективных протоколов защиты данных?
20. Какие риски необходимо учитывать при разработке процедур защиты информации?
21. Опишите один из кейсов успешной интеграции системы безопасности в бизнес-процесс.
22. Каковы общие характеристики успешных интеграций систем безопасности в бизнесе?
23. Какие факторы способствовали успеху интеграции модулей защиты в выбранном кейсе?
24. Каковы основные этапы моделирования сценариев атак на автоматизированные системы?
25. Какие типы атак чаще всего моделируются для оценки устойчивости АИС?
26. Как можно использовать результаты моделирования сценариев атак для улучшения безопасности системы?
27. Приведите примеры последствий успешной атаки на автоматизированную систему.
29. Какие основные правовые нормы регулируют вопросы несанкционированного доступа к информации?
29. Каковы этические аспекты, связанные с тестированием безопасности информационных систем?
30. В чем заключается ответственность за несанкционированный доступ к информации согласно законодательству?
31. Приведите примеры случаев, когда были нарушены этические нормы в области информационной безопасности.
32. Какие методы используются для повышения устойчивости автоматизированных систем к вредоносным программам?
33. Каковы основные принципы разработки защищенных АИС?
34. Какие технологии могут помочь в повышении устойчивости систем к специальным программным воздействиям?

Пример задания:

1. Какие основные этапы включает в себя процесс моделирования технологических процессов в АИС?
2. Каковы основные методы оценки статистической надежности результатов экспериментов?
3. Какие методы используются для повышения устойчивости автоматизированных систем к вредоносным программам?

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	Знает ответы на два вопроса или допускает ошибки в ответах на вопросы	Не отвечает на два и более вопросов

	собеседования		

7 Основная учебная литература

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

2. Ищейнов В. Я. Защита конфиденциальной информации : учебное пособие для студентов направления 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информации" / В. Я. Ищейнов, М. В. Мецатунян, 2011. - 254.

3. Глухов Н. И. Информационная безопасность предприятия [Электронный ресурс] : монография / Н. И. Глухов, 2008. - 197.

4. Глухих В. И. Информационная безопасность и защита данных : учебное пособие / В. И. Глухих, 2012. - 244.

5. Глухих В. И. Информационная безопасность и защита данных : учебное пособие для магистров по направлению "Информатика и вычислительная техника" / В. И. Глухих, 2012. - 276.

6. Глухих В. И. Информационная безопасность и защита данных : учебное пособие / В. И. Глухих, 2012. - 317.

7. Информационная безопасность и защита информации : учебное пособие для вузов по направлению "Информационные системы и технологии" / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова, Н. Г. Шахов, 2016. - 383.

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. Русаков С. А. Основы управленческой деятельности : учебное пособие для студентов высших учебных заведений / С. А. Русаков, 2008. - 240.

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. 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

17. 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

18. 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

19. МФУ FS-1128 MFP

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

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