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

«МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»

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: Дмитриев Алексей Александрович Дата подписания: 13.06.2026	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 14.06.2026	Документ подписан простой электронной подписью Согласовал: Маринов Александр Андреевич Дата подписания: 17.06.2026

Год набора – 2026

Иркутск, 2026 г.

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

1.1 Дисциплина «Методы оценки безопасности компьютерных систем» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ПКС-2 Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПКС-2.2
ПКС-3 Способность администрировать подсистемы информационной безопасности объекта защиты	ПКС-3.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПКС-2.2	Умеет проводить взаимосвязь функций и механизмов компьютерной безопасности, классифицировать компьютерные системы по уровню защищенности от несанкционированного доступа; владеет методами оценки систем безопасности (оранжевая книга «ОК», ITSEC, общие критерии оценки защищённости информационных технологий) взаимоотношением и взаимодействием между компонентами исследуемой системы	**Знать** Методы оценки защищенности компьютерных систем, требования к обеспечению безопасности информационных систем в США и России **Уметь** Формулировать критерии оценки безопасности информационных технологий **Владеть** Знанием для оценки ЗИ в АС системой показателей защищенности ИС и заданной иерархией классов безопасности, каждому из которых соответствует определенная совокупность обязательных функций ЗИ. Степень реализации выбранных критериев показывает текущее состояние безопасности. Последующие действия сводятся к сравнению реальных угроз с реальным состоянием безопасности.
ПКС-3.2	Способен определить источники угроз информационной безопасности при администрировании подсистемы информационной безопасности; умеет применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; владеет основными методами администрирования	**Знать** Методологии обеспечения безопасности систем и сетей предприятия, методы взаимодействия с внешней и внутренней средой, методы работ, анализ рисков, методы разработки, внедрения, эксплуатации и сопровождения, информационных систем в США и России. **Уметь** Формулировать критерии оценки безопасности

	безопасности компьютерных систем	информационных технологий **Владеть** Знанием для оценки ЗИ в АС системой показателей защищенности ИС и заданной иерархией классов безопасности, каждому из которых соответствует определенная совокупность обязательных функций ЗИ. Степень реализации выбранных критериев показывает текущее состояние безопасности. Последующие действия сводятся к сравнению реальных угроз с реальным состоянием безопасности.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Методы оценки безопасности компьютерных систем» базируется на результатах освоения следующих дисциплин/практик: «Информационные технологии», «Основы информационной безопасности», «Физические основы информационной безопасности», «Техническая защита информации»

Дисциплина является предшествующей для дисциплин/практик: «Основы управления информационной безопасностью»

3 Объем дисциплины

Объем дисциплины составляет – 3 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 7
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	64	64
лекции	32	32
лабораторные работы	0	0
практические/семинарские занятия	32	32
Самостоятельная работа (в т.ч. курсовое проектирование)	44	44
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет	Зачет

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 7

№ п/п	Наименование раздела и темы	Виды контактной работы			СРС	Форма текущего
		Лекции	ЛР	ПЗ(СЕМ)		

	дисциплины	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	**контроля**
1	2	3	4	5	6	7	8	9	10	11
1	АНАЛИЗ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ	1	6			1	5	1	7	Устный опрос
2	СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	2	2			2	5	1	7	Устный опрос
3	МОДЕЛЬ КОМПЛЕКСНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КС	3	6			3	6	1	7	Устный опрос
4	МЕТОДЫ КАЧЕСТВЕННОЙ ОЦЕНКИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	4	6			4	5	1	8	Устный опрос
5	МЕТОДЫ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ	5	6			5	5	1	7	Устный опрос
6	КОМПЛЕКСНЫЙ ПОДХОД К ОЦЕНКЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ	6	6			6	6	1	8	Устный опрос
	Промежуточная аттестация									Зачет
	Всего		32				32		44	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 7

№	Тема	Краткое содержание
1	АНАЛИЗ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ	Сущность коммерческой тайны и необходимость ее защиты Анализ угроз безопасности Неформальная модель нарушителя
2	СТАНДАРТЫ ИНФОРМАЦИОННОЙ	Первые стандарты безопасности Стандарт ISO/IEC 15408

	БЕЗОПАСНОСТИ	Международный стандарт ISO 17799 Российские стандарты безопасности Гармонизированные критерии Европейских стран
3	МОДЕЛЬ КОМПЛЕКСНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КС	Формальная модель КСИБ Механизм функционирования КСИБ
4	МЕТОДЫ КАЧЕСТВЕННОЙ ОЦЕНКИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	Оценка уровня информационной безопасности Оценка рисков Тестирование систем информационной безопасности
5	МЕТОДЫ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ	Метод экспертных оценок Метод информационных потоков Графовый метод Метод весовых коэффициентов
6	КОМПЛЕКСНЫЙ ПОДХОД К ОЦЕНКЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ	Оценка экономической эффективности КСИБ

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 7

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Контрольные вопросы по лекции №1	5
2	Контрольные вопросы по лекции №2	5
3	Контрольные вопросы по лекции №3	6
4	Контрольные вопросы по лекции №4	5
5	Контрольные вопросы по лекции №5	5
6	Контрольные вопросы по лекции №6	6

4.5 Самостоятельная работа

Семестр № 7

№	Вид СРС	Кол-во академических часов
1	Тестирование по разделам дисциплин	44

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Мозговой штурм

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

Торокин А.А. Инженерно-техническая защита информации: Учебное пособие. - М.: Гелиос-АРВ, 2005.
Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие. – М.: Издательский центр «Академия», 2005. – 144 с.

5.1.2 Методические указания для обучающихся по самостоятельной работе:

Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации, Москва: Книжный дом «Либроком», 2013.
Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. - М.: Горячая линия, 2005.

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 7 | Устный опрос

Описание процедуры.

1. Выдача 2 вопросов каждому студенту индивидуально
2. Подготовка студентами письменного ответа
3. Объяснения ответов на вопросы

Критерии оценивания.

Глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, использует в ответе материал научной литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.

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
ПКС-2.2	Способен подобрать аналитические и компьютерные модели автоматизированных систем и систем защиты информации	Устное собеседование по теоретическим вопросам и/или выполнение

		практических заданий
ПКС-3.2	Способен подобрать аналитические и компьютерные модели автоматизированных систем и систем защиты информации	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 7, Типовые оценочные средства для проведения зачета по дисциплине

6.2.2.1.1 Описание процедуры

Успешному проведению зачета способствует систематическое посещение лекционных, практических и семинарских занятий, тщательная проработка вопросов, выносимых на обсуждения на групповых занятиях, и самостоятельная подготовка обучающихся. При подготовке к зачету необходимо ознакомиться с вопросами, составить структурно-логическую схему ответа на каждый вопрос, используя при этом материалы лекционных практических и семинарских занятий, рекомендуемую преподавателем литературу. При возникновении сложностей в процессе подготовки к зачету необходимо обратиться за консультацией к преподавателю. Зачет является заключительным этапом изучения учебной дисциплины и имеет целью проверить теоретические знания обучающихся, их навыки и умение применять полученные знания при решении практических задач. Зачет проводится в объеме рабочей программы учебной дисциплины

Пример задания:

1. Особенности современных автоматизированных систем.
2. Требования к системам и средствам защиты информации от несанкционированного доступа.
3. Классификация автоматизированных систем и требования по защите информации.
4. Показатели защищенности средств вычислительной техники.
5. Соответствие классов систем различным уровням конфиденциальности.
6. Понятие модели нарушителя информационной безопасности и модели угроз информационной безопасности.
7. Политика безопасности.
8. Принципы построения системы защиты информации.
9. Определение уязвимостей автоматизированных систем и выбор средств защиты.
10. Формирование требований к построению систем защиты.
11. Создание автоматизированных систем в защищенном исполнении.
12. Классификация каналов утечки информации.
13. Методы защиты речевой информации.
14. Методы защиты информации от утечки за счет побочных электромагнитных излучений и наводок.
15. Специальные проверки и специальные исследования оборудования.
16. Противодействие наблюдению в оптическом диапазоне.
17. Инженерно-техническая защита информации.

18. Методы противодействия разведкам.
19. Методы контроля доступа к ресурсам компьютерной системы.
20. Модели безопасности компьютерных систем.
21. Дискреционные модели безопасности: модель Харрисона-Рузо-Ульмана.
22. Модель типизированных матриц доступа.
23. Модель take-grant.
24. Мандатное управление доступом.
25. Модель Белла-Лападулы.
26. Модель LWM.
27. Автоматная модель невлияния.
28. Методы поиска остаточной информации на машинных носителях.
29. Методы гарантированного удаления информации.
30. Сущность разрушающих программных воздействий.
31. Модели взаимодействия прикладных программ и программы-злоумышленника, классификация разрушающих программных средств.
32. Компьютерные вирусы. Принципы и методы защиты от разрушающих программных воздействий.
33. Уязвимости приложений: атаки типа переполнение буфера, стека и кучи, атаки, основанные на изменении входных данных.
34. Атаки на web-приложения: атаки типа SQL-инъекция и межсайтовый скриптинг.
35. Безопасность сокетов.
36. Безопасность ActiveX-элементов, DCOM-объектов и RPC-элементов.
37. Атаки типа «отказ в обслуживании».
38. Требования ФСТЭК России к программному обеспечению средств защиты и его классификация по уровню отсутствия недекларирован-ных возможностей.
39. Виртуальные частные сети. Криптографическая защита трафика на всех уровнях модели ISO/OSI.
40. Криптографическая защиты сетевого уровня. Семейство протоколов IPsec и его модификации.
41. Средства криптографической защиты прикладного уровня. Протокол SSL/TLS.
42. Протокол RADIUS, протокол Kerberos.
43. Проблема разграничения доступа в компьютерных сетях. Понятие межсетевого экрана.
44. Виды межсетевых экранов. Принципы работы межсетевых экранов.
45. Уязвимости основных протоколов сетевого взаимодействия.
46. Понятие системы обнаружения вторжений и ее функции. Основные методы детектирования атак.

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено
Имеет знания основного материала, допускаются некоторые неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, возможны некоторые затруднения при выполнении практических работ	Не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы

7 Основная учебная литература

1. Громкович Ю. Теоретическая информатика. Введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию : учебник / Ю. Громкович, 2010. - 325.

2. Баричев С. Г. Основы современной криптографии [Электронный ресурс] / С. Г. Баричев, Р. Е. Серов, 2002. - 152.

[Сайт] – URL: http://elib.istu.edu/viewer/view.php?file=/files/er-0079.pdf

8 Дополнительная учебная литература и справочная

1. Грушо А. А. Теоретические основы компьютерной безопасности : учебное пособие для вузов по специальностям группы 090100 "Информационная безопасность" / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина, 2009. - 267.

2. Девянин П. Н. Модели безопасности компьютерных систем : учеб. пособие для вузов по специальностям 075200 "Компьютер. безопасность" / П. Н. Девянин, 2005. - 142.

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. Лицензионное программное обеспечение Системное программное обеспечение

2. Лицензионное программное обеспечение Пакет прикладных офисных программ

3. Лицензионное программное обеспечение Интернет-браузер

12 Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения лекционных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оснащение: комплект учебной мебели, рабочее место преподавателя, доска. Мультимедийное оборудование (в том числе переносное): мультимедийный проектор, экран, акустическая система, компьютер с выходом в интернет.

2. Учебная аудитория для проведения лабораторных/практических (семинарских) занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оснащение: комплект учебной мебели, рабочее место преподавателя, доска.

Мультимедийное оборудование (в том числе переносное): мультимедийный проектор, экран, акустическая система, компьютер с выходом в интернет.