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

«ТЕХНОЛОГИЯ СОЗДАНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

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: 17.06.2026	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 «Технология создания защищенных информационных систем» 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-6.5

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПК-6.5	Разрабатывает техническое задание на создание автоматизированной системы, включая модели угроз нарушителя; разрабатывает на их основе модели информационной системы в защищенном исполнении	**Знать** существующую нормативно-методическую базу в области информационной безопасности; состав, структуру и назначение нормативно-методических документов ФСТЭК России; принципы выбора и учета требований нормативно-методических документов в своей профессиональной деятельности. **Уметь** формировать требования к объектам информационных технологий с учетом требований нормативно-методических документов в области информационной безопасности; оценивать полноту реализации в продуктах информационных технологий требований нормативно-методических документов в области информационной безопасности. **Владеть** инструментальными средствами проверки реализации требований нормативно-методических документов в области информационной безопасности.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Технология создания защищенных информационных систем» базируется на результатах освоения следующих дисциплин/практик: «Защищенные информационные системы»

Дисциплина является предшествующей для дисциплин/практик: «Разработка и стандартизация программных средств и информационных технологий»

3 Объем дисциплины

Объем дисциплины составляет – 2 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 3
Общая трудоемкость дисциплины	72	72
Аудиторные занятия, в том числе:	26	26
лекции	13	13
лабораторные работы	0	0
практические/семинарские занятия	13	13
Самостоятельная работа (в т.ч. курсовое проектирование)	46	46
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 № 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	Концептуальная канва формирования нормативно-методического обеспечения информационной безопасности	1	2			1	2	1	7	Устный опрос
2	Технологическая канва формирования нормативно-методического обеспечения информационной безопасности	2	2			2	2	1	7	Устный опрос
3	Нормативно-методическое обеспечение защиты от несанкционированного доступа к информации	3	2			3	2	1	8	Устный опрос
4	Нормативно-методическое	4	2			4	2	1	8	Устный опрос

	обеспечение безопасности персональных данных									
5	Нормативно-методическое обеспечение безопасности информационных технологий	5	2			5	2	1	8	Устный опрос
6	Нормативно-методическое обеспечение информационной безопасности сетевых технологий.	6	3			6	3	1	8	Устный опрос
	Промежуточная аттестация									Зачет
	Всего		13				13		46	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 3

№	Тема	Краткое содержание
1	Концептуальная канва формирования нормативно-методического обеспечения информационной безопасности	Рассматриваются базовые понятия, которыми необходимо овладеть в рамках учебной дисциплины. Рассматриваются критерии защищенности информационных систем и основополагающие начала их построения.
2	Технологическая канва формирования нормативно-методического обеспечения информационной безопасности	Рассматриваются вопросы структурного построения компьютерных систем. Уделяется внимание особенностям построения систем на основе баз данных, изучаются специфика технологии их проектирования.
3	Нормативно-методическое обеспечение защиты от несанкционированного доступа к информации	Изучаются основы разграничения доступа в процессе построения защищенных компьютерных систем.
4	Нормативно-методическое обеспечение безопасности персональных данных	Рассматриваются различные альтернативные варианты обеспечения целостности компьютерных систем, созданных на основе баз данных, изучаются средства обеспечения их конфиденциальности.
5	Нормативно-методическое обеспечение безопасности информационных	Рассматриваются принципы защищенного хранения информации и средства, позволяющие реализовывать указанную задачу.

	технологий	
6	Нормативно-методическое обеспечение информационной безопасности сетевых технологий.	Изучаются отдельные группы методов защиты информации, изучаются вопросы их применения в комплексе.

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	Основные понятия защищенных информационных систем. Общие принципы построения защищенных информационных систем	2
2	Архитектура информационных систем на основе баз данных. Технологии проектирования баз данных.	2
3	Разграничения доступа к ресурсам информационной системы	2
4	Средства обеспечения целостности информационных систем на основе баз данных. Средства обеспечения конфиденциальности информации в системах на основе баз данных	2
5	Способы хранения конфиденциальной информации.	2
6	Основные направления защиты информации. Организационные меры защиты информации в организации.	3

4.5 Самостоятельная работа

Семестр № 3

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	46

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/course/view.php?id=7963

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/course/view.php?id=7963

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.

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-6.5	Демонстрирует навыки оформления инженерной и проектно-конструкторской документации, может оформить рабочую техническую документацию на различных этапах жизненного цикла СЗИ.	Устное собеседование по теоретическим вопросам и индивидуальным практическим занятиям

6.2.2 Типовые оценочные средства промежуточной аттестации

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

6.2.2.1.1 Описание процедуры

В ходе зачета студент должен быть готов к ответу на дополнительные вопросы, к решению задач в рамках проблематики билета. При подготовке к ответу на вопрос на зачете можно использовать программу курса и, если это согласовано с преподавателем, нормативные источники.
Зачет проводится в аудитории, которая заранее определяется учебным отделом. Для

подготовки к сдаче зачета студенту может быть выдана рабочая программа по дисциплине. Студентам предъявляются на выбор билеты зачета, включающие два вопроса. Преподаватель вправе предложить студенту практическую задачу в качестве третьего задания

Зачет проводится в устной форме. Однако студентам рекомендуется сделать краткие записи ответов на проштампованных листах. Письменные ответы делаются в произвольной форме. Это может быть развернутый план ответов, статистические данные, точные формулировки нормативных актов, схемы, позволяющие иллюстрировать ответ, и т.п. Записи, сделанные при подготовке к ответу, позволят студенту составить план ответа на вопросы, и, следовательно, полно, логично раскрыть их содержание, а также помогут отвечающему справиться с естественным волнением, чувствовать себя увереннее. В то же время записи не должны быть слишком подробные. В них трудно ориентироваться при ответах, есть опасность упустить главные положения, излишней детализации несущественных аспектов вопроса, затянуть его. В итоге это может привести к снижению уровня ответа и повлиять на его оценку.

Зачет проводится в форме устного опроса по билетам.

1. Определение требований к системе защиты информации.
2. Информационные технологии и необходимость ИБ.
3. Система защиты информации и ее структуры.
4. Экономическая информация как товар и объект безопасности.
5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для компании.
10. Информационные угрозы для личности (физического лица).
11. Действия и события, нарушающие информационную безопасность.
12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
13. Способы воздействия информационных угроз на объекты.
14. Внешние и внутренние субъекты информационных угроз.
15. Компьютерные преступления и их классификация.
16. Исторические аспекты компьютерных преступлений и современность.
17. Субъекты и причины совершения компьютерных преступлений.
18. Вредоносные программы, их виды.
19. История компьютерных вирусов и современность.
20. Деятельность международных организаций в сфере информационной безопасности.
21. Государственное регулирование информационной безопасности в РФ.
22. Задачи ИБ в программе « цифровая экономика».
23. Доктрина информационной безопасности России.
24. Федеральные законы в сфере информатизации и информационной безопасности в РФ.
25. Уголовно-правовой контроль над компьютерной преступностью в РФ.
26. Политика безопасности и ее принципы.
27. Фрагментарный и системный подход к защите информации.
28. Методы и средства защиты информации.
29. Организационное обеспечение ИБ.
30. Каким образом принимается решение о необходимости создания системы защиты информации.
31. Организация конфиденциального делопроизводства.

Пример задания:

1. Определение требований к системе защиты информации
2. Работа регулятора в области защиты информации.

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено
Ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений. Полно раскрываются причинно-следственные связи между государственными, политическими и правовыми явлениями и событиями. Делаются обоснованные выводы. Демонстрируются глубокие знания базовых нормативно-правовых актов. Соблюдаются нормы литературной речи. Проанализированы различные точки зрения авторов.	Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Не раскрываются причинно-следственные связи между государственными, политическими и правовыми явлениями и событиями. Не проводится анализ. Выводы отсутствуют. Имеются заметные нарушения норм литературной речи.

7 Основная учебная литература

1. Воробьев Л. В. Системы и сети передачи информации : учебное пособие для вузов по специальностям "Компьютерная безопасность" / Л. В. Воробьев, А. В. Давыдов, Л. П. Щербина, 2009. - 328.

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

8 Дополнительная учебная литература и справочная

1. Ярочкин Владимир Иванович. Безопасность информационных систем / Владимир Иванович Ярочкин; Попечит. Совет правоохран. органов г. Москвы, 1996. - 318.

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, 2009. - 330.

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. МФУ FS-1128 MFP

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

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