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

«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА 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: 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 «Программно-аппаратные средства защиты информации» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК ОС-9 Способность применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК ОС-9.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-9.2	Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**Знать** процесс установки, настройки и обслуживанию программных, программно-аппаратных (в том числе криптографических) комплексов, а также подсистемы информационной безопасности объекта защиты. **Уметь** администрировать программные средства системы защиты информации автоматизированных систем; - уметь устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации; - уметь проводить анализ структурных и функциональных схем защищенной автоматизированной системы; - уметь определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы. **Владеть** программными средствами системного, прикладного и специального назначения, языками программирования для решения профессиональных задач.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Программно-аппаратные средства защиты информации» базируется на результатах освоения следующих дисциплин/практик: «Языки

программирования», «Нейронные сети», «Комплексная система защиты информации на предприятии», «Методы и средства криптографической защиты информации»

Дисциплина является предшествующей для дисциплин/практик: «Основы управления информационной безопасностью», «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 № 7
Общая трудоемкость дисциплины	144	144
Аудиторные занятия, в том числе:	64	64
лекции	16	16
лабораторные работы	32	32
практические/семинарские занятия	16	16
Самостоятельная работа (в т.ч. курсовое проектирование)	44	44
Трудоемкость промежуточной аттестации	36	36
Вид промежуточной аттестации (итогового контроля по дисциплине)	Экзамен, Курсовая работа	Экзамен, Курсовая работа

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 7

№ 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	Подсистемы защиты современных операционных систем	1	3	1	6	1	3	1	8	Устный опрос
2	Защита информации в компьютерных сетях	2	3	2	6	2	3	1	7	Устный опрос
3	Защита информации в системах управления базами данных.	3	3	3	5	3	3	1	7	Устный опрос
4	Антивирусная защита компьютерных систем.	4	3	4	6	4	3	1	10	Устный опрос

5	Административный уровень обеспечения информационной безопасности	5	2	5	4	5	2	1	6	Устный опрос
6	Обеспечение режима конфиденциальности при работе с защищаемой информацией	6	2	6	5	6	2	1	6	
	Промежуточная аттестация								36	Экзамен, Курсовая работа
	Всего		16		32		16		80	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 7

№	Тема	Краткое содержание
1	Подсистемы защиты современных операционных систем	Субъекты, объекты, методы и права доступа в современных операционных системах. Основные компоненты подсистем защиты UNIX и Windows. Управление доступом, аутентификация, аудит. Основные проблемы с безопасностью и возможные решения в современных операционных системах. Аудит информационной безопасности.
2	Защита информации в компьютерных сетях	Обеспечение безопасности межсетевого взаимодействия. Атаки на сетевые службы, типы угроз, классификация атак по основным механизмам реализации угроз. Сетевые сканеры. Адаптивная безопасность в вычислительных сетях. Пакетные фильтры и межсетевые экраны, их классификация и особенности применения. Виртуальные частные сети. Системы обнаружения атак и вторжений.
3	Защита информации в системах управления базами данных.	Угрозы безопасности баз данных: общие и специфичные. Модели безопасности систем управления базами данных (СУБД). Средства и методы обеспечения целостности данных в СУБД. Ролевое разграничение доступа к данным в современных СУБД.
4	Антивирусная защита компьютерных систем.	Понятие вредоносной программы и их классификация. Принципы построения политики безопасности, обеспечивающей высокую защищенность от вредоносного программного обеспечения: принцип минимизации программного обеспечения, принцип минимизации полномочий пользователей. Специализированные средства и методы выявления вредоносных программ: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных

		потоков, изолированная программная среда, программные ловушки.
5	Административный уровень обеспечения информационной безопасности	Концепция информационной безопасности, её цели и этапы построения. Политика информационной безопасности как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику безопасности, и основные этапы разработки политики информационной безопасности. Задачи, решаемые при анализе рисков. Базовые методики, используемые для оценки рисков. Основные стандарты в области разработки политики информационной безопасности и анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации политики информационной безопасности.
6	Обеспечение режима конфиденциальности при работе с защищаемой информацией	Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиденциальным сведениям, документам и базам данных. Допуск должностных лиц, работников к конфиденциальной информации. Доступ должностных лиц, работников к конфиденциальным сведениям, документам и базам данных. Обязанности должностных лиц, допущенных к сведениям, составляющим коммерческую тайну. Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям.

4.3 Перечень лабораторных работ

Семестр № 7

№	Наименование лабораторной работы	Кол-во академических часов
1	Защиты современных операционных систем	6
2	Защита информации в компьютерных сетях	6
3	Системы управления базами данных	5
4	Антивирусная защита компьютерных систем	6
5	Уровни обеспечения информационной безопасности	4
6	Режим конфиденциальности при работе с защищаемой информацией	5

4.4 Перечень практических занятий

Семестр № 7

№	Темы практических (семинарских) занятий	Кол-во академических

		часов
1	Субъекты, объекты, методы и права доступа в современных операционных системах.	3
2	Атаки на сетевые службы, типы угроз, классификация атак по основным механизмам реализации угроз.	3
3	Модели безопасности систем управления базами данных (СУБД)	3
4	Специализированные средства и методы выявления вредоносных программ	3
5	Базовые инструментальные средства для анализа рисков и управления рисками ИБ	2
6	Допуск должностных лиц, работников к конфиденциальной информации	2

4.5 Самостоятельная работа

Семестр № 7

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям (лабораторным работам)	44

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: в теоретическом курсе предусматривается проведение интерактивной лекции по темам: «Подсистемы защиты современных операционных систем», «Обеспечение режима конфиденциальности при работе с защищаемой информацией», «Программно-аппаратные средства защиты информации в сфере информационной безопасности» (Темы №3,4,5); при проведении практических работ предусматривается решение задач по расчетам экономических показателей, а также проведение при решении задач по индивидуальным заданиям «разбора конкретных ситуаций».

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по курсовому проектированию/работе:

https://el.istu.edu/

5.1.2 Методические указания для обучающихся по практическим занятиям

https://el.istu.edu/

5.1.3 Методические указания для обучающихся по лабораторным работам:

https://el.istu.edu/

5.1.4 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 7 | 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
ОПК ОС-9.2	отлично; хорошо; удовлетворительно; неудовлетворительно	устное собеседование по теоретическим вопросам

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 7, 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 три вопроса в билете.
Экзамен проводится в форме устного опроса по экзаменационным билетам

6.2.2.1.2 Критерии оценивания

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Уверенно и без ошибок отвечает	Допускает незначительные	Знает ответы на два вопроса или	Не отвечает на два и более вопросов.

на все вопросы билета.	ошибки в ответе на один из вопросов, включая дополнительные по результатам собеседования.	допускает ошибки в ответах на вопросы.	

6.2.2.2 Семестр 7, Типовые оценочные средства для курсовой работы/курсового проектирования по дисциплине

6.2.2.2.1 Описание процедуры

Курсовая работа по дисциплине является одним из основных видов учебных занятий и формой контроля учебной работы обучающихся.
Выполнение обучающимся курсовой работы осуществляется на заключительном этапе изучения учебной дисциплины, в ходе которого осуществляется обучение применению полученных знаний и умений при решении комплексных задач, связанных со сферой профессиональной деятельности будущих специалистов.
Выполнение обучающимся курсовой работы по дисциплине проводится с целью:
- систематизации и закрепления полученных теоретических знаний и практических умений по общепрофессиональным и специальным дисциплинам;
- углубления теоретических знаний в соответствии с заданной темой;
- формирования умений применять теоретические знания при решении поставленных вопросов;
- формирование умений использовать справочную, нормативную и правовую документацию; развития творческой инициативы, самостоятельности, ответственности и организованности; подготовки к итоговой государственной аттестации.

Разработка тематики курсовых работ. Типовая тематика курсовых работ указывается в рабочей программе дисциплины. Обучающимся предоставляется право выбора темы курсовой работы в соответствии с типовой тематикой.
В соответствии с типовой тематикой курсовых работ преподавателями «Центра компетенций по кибербезопасности» ежегодно разрабатывается тематика курсовых работ по учебным группам, рассматривается на заседании «Центра компетенций по кибербезопасности» и утверждается на заседании УМК Института ИТ и АД не позднее, чем за месяц до начала курсового проектирования.
Тема курсовой работы может быть предложена обучающимся при условии обоснования им ее целесообразности. Задание на курсовое проектирование выдается каждому обучающемуся, независимо от текущей оценки по дисциплине в срок не позднее, чем за две недели до начала курсового проектирования.
Оформление курсовой работы должно соответствовать требованиям, прописанным в методических рекомендациях.

Пример задания:

Типовая тематика курсовых работ:

1. Анализ технологии VPN и ее построение.
2. Компьютерные преступления и методы защиты информации.
3. Обеспечение информационной безопасности при дистанционном обучении.

4. Организация защиты информации в локальной вычислительной сети.
5. Использование услуг IT аутсорсинга при обеспечении информационной безопасности организации.
6. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему.
7. Анализ защищенности информационной безопасности на воздушном транспорте
8. Методы и средства защиты информации от несанкционированного доступа. Методы и средства защиты от компьютерных вирусов.
9. Организация безопасности сети предприятия с использованием операционной системы Linux.
10. Разработка и анализ информационной системы безопасности для системы управления производством.
11. Методы и средства защиты информации в сетях.
12. Процесс обработки и защиты персональных данных онлайн-платформами.
13. Исследование внешних угроз информационной безопасности.
14. Промышленный шпионаж как один из видов нарушения информационной безопасности.
15. Анализ уязвимостей программного обеспечения.
16. Анализ и разработка информационной системы для объектов критической информационной инфраструктуры.
17. Способы и методы защиты информационных ресурсов.
18. Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей.
19. Роль специалиста по защите информации для экономики России.
20. Методы обеспечения безопасности интернет-ресурсов.
21. Сущность, назначение и структура системы защиты информации.
22. Механизмы защиты информации в вычислительных сетях.
23. Защита информации сети предприятия средствами Secret net.
24. Стандарты и сертификации в области информационной безопасности.
25. Технологии защиты информации в WI-FI сетях.
26. Разработка новых алгоритмов электронной подписи и их сравнительный анализ с известными стандартами.
27. Сущность, назначение и структура системы защиты информации.
28. Система инженерно-технической защиты информации.
29. Защита от SQL-атак.

6.2.2.2.2 Критерии оценивания

Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
- получают обучающиеся, оформившие курсовую работу в соответствии с предъявляемыми требованиями, в которой отражены все необходимые результаты	- получают обучающиеся, оформившие курсовую работу в соответствии с предъявляемыми требованиями, в которой отражены все необходимые результаты	- получают обучающиеся, оформившие курсовую работу в соответствии с предъявляемыми требованиями. При этом при ответах на вопросы преподавателя	- ставится за курсовую работу, если число ошибок и недочетов превысило удовлетворительный уровень компетенции. Элементы компетенций не сформированы.

проведенного анализа, сделаны обобщающие выводы и предложены рекомендации в соответствии с тематикой курсовой работы, а также грамотно и исчерпывающе ответившие на все встречные вопросы преподавателя. Элементы компетенций сформированы на высоком уровне.	проведенного анализа, сделаны обобщающие выводы и предложены рекомендации в соответствии с тематикой курсовой работы. При этом при ответах на вопросы преподавателя обучающийся допустил не более двух ошибок. Элементы компетенций в основном сформированы на среднем, но достаточно высоком уровне.	обучающийся допустил более трёх ошибок. Элементы компетенций сформированы на достаточном, но минимальном пороговом уровне.	

7 Основная учебная литература

1. Методические указания по проведению лабораторных работ по дисциплине "Техническая защита информации" по теме "Методы обнаружения скрытых видеокамер" [Электронный ресурс] : для студентов по направлению подготовки/специальности 10.03.01 "Информационная безопасность" / Иркут. нац. исслед. техн. ун-т, Каф. информ. безопасности, 2018. - 22.

2. Методические указания по проведению лабораторных работ по дисциплине "Техническая защита информации" по теме "Защита информации от утечки по цепям электропитания" [Электронный ресурс] : для студентов по направлению подготовки/специальности 10.03.01 "Информационная безопасность" / Иркут. нац. исслед. техн. ун-т, Ин-т высоких технологий, Каф. информ. безопасности, 2018. - 30.

3. Хорев П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев, 2012. - 351.

4. 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. Методические указания по проведению лабораторных работ по дисциплине "Техническая защита информации" по теме "Выявление каналов утечки информации за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах" [Электронный ресурс] : для студентов по направлению

подготовки/специальности 10.03.01 "Информационная безопасность" / Иркут. нац. исслед. техн. ун-т, Каф. информ. безопасности, 2018. - 22.

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. 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