Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Брикс кафедра»

УТВЕРЖДЕНА:
на заседании кафедры
Протокол №15 от 18 марта 2025 г.

Рабочая программа дисциплины

«ЗАЩИТА ИНФОРМАЦИИ / INFORMATION SECURITY»

Направление: 09.03.01 Информатика и вычислительная техника

Искусственный интеллект и компьютерные науки /Artificial Intelligence and Computer Science

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Усов Евгений Геннадьевич Дата подписания: 18.06.2025	Документ подписан простой электронной подписью Утвердил: Киреенко Анна Павловна Дата подписания: 19.06.2025	Документ подписан простой электронной подписью Согласовал: Афанасьев Александр Диомидович Дата подписания: 18.06.2025

Год набора – 2025

Иркутск, 2025 г.

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

1.1 Дисциплина «Защита информации / Information Security» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК ОС-10 Способность применять методы и средства защиты информации	ОПК ОС-10.3, ОПК ОС-10.2
ОПК ОС-3 Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК ОС-3.2, ОПК ОС-3.3

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-3.2	Имеет представление об основных компонентах информационной безопасности и способен применять инструменты обеспечения информационной безопасности в рамках решения задач профессиональной деятельности	**Знать** **Уметь** **Владеть**
ОПК ОС-10.3	Способен определять угрозы безопасности информации в своей профессиональной деятельности	**Знать** **Уметь** **Владеть**
ОПК ОС-3.3	Применяет профессиональные знания на практике для решения стандартных задач профессиональной деятельности согласно требованиям информационной безопасности	**Знать** **Уметь** **Владеть**
ОПК ОС-10.2	Способен применить методы и средства защиты информации для защиты программного и аппаратного обеспечения компьютеров	**Знать** Основные угрозы информационной безопасности программного и аппаратного обеспечения. Принципы работы современных методов и средств защиты информации (криптография, антивирусы, межсетевые экраны, системы обнаружения вторжений и др.). Нормативно-правовую базу в

		области защиты информации (ФЗ «О персональных данных», ФЗ «Об информации, информационных технологиях и о защите информации» и др.). Классификацию атак на программное и аппаратное обеспечение и способы их предотвращения. Основные стандарты и протоколы информационной безопасности (ISO 27001, PCI DSS, TLS/SSL и др.). **Уметь** Применять методы криптографической защиты данных (шифрование, электронная подпись, хеширование). Настраивать и администрировать средства защиты информации (антивирусы, VPN, IDS/IPS, SIEM-системы). Анализировать уязвимости программного и аппаратного обеспечения с использованием специализированных инструментов (Nmap, Metasploit, Wireshark и др.). Разрабатывать и внедрять политики информационной безопасности для защиты компьютеров и сетей. Обеспечивать безопасность операционных систем и приложений с помощью настройки прав доступа, обновлений и мониторинга. **Владеть** Навыками работы с инструментами защиты информации (настройка межсетевых экранов, антивирусного ПО, систем мониторинга). Методами тестирования на проникновение (penetration testing) и оценки защищенности систем. Практическим опытом реагирования на инциденты информационной

		безопасности. Умением разрабатывать рекомендации по повышению уровня защиты ПО и аппаратного обеспечения. Способностью выбирать оптимальные средства защиты в зависимости от типа угроз и характеристик защищаемой системы.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Защита информации / Information Security» базируется на результатах освоения следующих дисциплин/практик: «Введение в специальность / Introduction to the specialty», «Программирование / Programming»

Дисциплина является предшествующей для дисциплин/практик: «Технологии внедрения решений искусственного интеллекта / Artificial Intelligence Implementation Technologies»

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 № 6
Общая трудоемкость дисциплины	144	144
Аудиторные занятия, в том числе:	72	72
лекции	36	36
лабораторные работы	0	0
практические/семинарские занятия	36	36
Самостоятельная работа (в т.ч. курсовое проектирование)	36	36
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 № 6

№ 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	Введение в информационную безопасность	1	6			1	6	1	6	Устный опрос
2	Криптографические методы защиты информации	2	6			2	6	1	6	Устный опрос
3	Защита программного обеспечения	3	6			3	6	1	6	Устный опрос
4	Защита сетевой инфраструктуры	4	6			4	6	1	6	Устный опрос
5	Аппаратные средства защиты информации	5	6			5	6	1	6	Устный опрос
6	Управление информационной безопасностью	6	6			6	6	1	6	Устный опрос
	Промежуточная аттестация								36	Экзамен
	Всего		36				36		72	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 6

№	Тема	Краткое содержание
1	Введение в информационную безопасность	Основные понятия: конфиденциальность, целостность, доступность (CIA-триада). Угрозы и уязвимости информационных систем. Нормативно-правовая база
2	Криптографические методы защиты информации	Основы криптографии: симметричное и асимметричное шифрование. Алгоритмы (AES, RSA, ГОСТ 34.10-2012). Электронная подпись и хеширование (SHA, MD5).
3	Защита программного обеспечения	Уязвимости ПО и методы их устранения. Антивирусные системы и sandbox-анализ. Безопасная разработка (Secure SDLC, OWASP Top 10).
4	Защита сетевой инфраструктуры	Межсетевые экраны (firewalls), IDS/IPS-системы. VPN и защищенные протоколы (TLS/SSL, SSH). Анализ сетевых атак (DDoS, MITM, фишинг).
5	Аппаратные средства защиты информации	Trusted Platform Module (TPM), HSM-модули. Защита от side-channel атак.

		Биометрические системы аутентификации.
6	Управление информационной безопасностью	Политики безопасности и регламенты (BYOD, DLP). Аудит и мониторинг (SIEM, SOC). Инцидент-менеджмент и расследование киберинцидентов.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 6

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Введение в информационную безопасность	6
2	Криптографические методы защиты информации	6
3	Защита программного обеспечения	6
4	Защита сетевой инфраструктуры	6
5	Аппаратные средства защиты информации	6
6	Управление информационной безопасностью	6

4.5 Самостоятельная работа

Семестр № 6

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	36

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Дискуссия; Деловая игра; Кейс-метод; Лекция с ошибками; Мозговой штурм; Тренинг; Отдельные занятия по курсу могут проводиться в форме активного практического обучения: выездных занятий с посещением организаций и мероприятий для получения новых знаний и/или повторения материала на практике. При проведении таких занятий преподаватель выступает в качестве помощника и координатора процесса, передавая активную функцию обучения студентам. Он же регулирует процесс посредством подготовки специальных заданий, проведения консультаций, оценки знаний, умений и навыков, предоставления обратной связи. Помимо получения знаний активные практические занятия развивают коммуникативные навыки, учат студентов работать в команде, решать проблемы.

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

Доклад — это устное выступление (5–7 минут) с презентацией, раскрывающее конкретный аспект темы.

Как готовиться:

Выберите актуальный аспект: Например, не просто «Экономика России», а «Роль IT-сектора в импортозамещении».

Соберите данные: Используйте статистику (Росстат), новости (ТАСС, РИА Новости), научные статьи.

Создайте презентацию:

Слайды должны быть лаконичными (1 идея = 1 слайд).

Добавьте графики, фото, схемы для наглядности.

Проговорите речь: Репетируйте, чтобы уложиться в время и уверенно отвечать на вопросы.

5.1.2 Методические указания для обучающихся по самостоятельной работе:

Курс направлен на формирование у вас системного понимания современной российской государственности, её политических, правовых, экономических и культурных особенностей. Для успешного освоения дисциплины и эффективной подготовки к практическим занятиям (эссе, докладам, устным опросам) следуйте этим рекомендациям.
Общие советы
Работайте с источниками: Официальные сайты (kremlin.ru, government.ru), научные журналы («Полис», «Россия в глобальной политике»).

Участвуйте в дискуссиях: На семинарах задавайте вопросы, сравнивайте Россию со своей страной.

Используйте мультимедиа: Документальные фильмы (например, «Россия глазами иностранцев»), подкасты («Медуза» о политике).

Важно! Даже если тема кажется сложной (например, «Судебная система РФ»), ищите простые аналогии: «Арбитражный суд — как футбольный арбитр для бизнеса».
1. Подготовка к эссе
Эссе предполагает краткое, но содержательное изложение вашей позиции по заданной теме с аргументацией.

Как готовиться:

Изучите тему: Используйте материалы лекций, рекомендованную литературу и официальные источники (Конституция РФ, сайты государственных органов).

Определите структуру: Введение (постановка проблемы), основная часть (аргументы + примеры), заключение (выводы).

Пишите четко: Избегайте общих фраз, опирайтесь на факты (например, не «Россия большая страна», а «РФ включает 89 субъектов, что обеспечивает разнообразие

экономических условий»).

Проверьте уникальность: Цитируйте источники корректно, не допускайте плагиата.

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 6 | Устный опрос

Описание процедуры.

1. Цель
Проверить глубину понимания материала, способность логично излагать мысли, аргументировать позицию и применять знания в практических ситуациях.

2. Подготовка к устному ответу

Повторите ключевые темы:

Основные понятия

Структура власти

Актуальные вопросы

Изучите рекомендованные источники

3. Проведение устного ответа

Формат:

Индивидуальный (ответ на 1–2 вопроса с последующим диалогом с преподавателем).

Групповой (дискуссия по проблемному вопросу)

Этапы:

Выбор вопроса:

Студент вытягивает билет или получает вопрос от преподавателя.

Возможна подготовка (3–5 минут для составления плана ответа).

Основной ответ (2–3 минуты):

Четкая структура: определение понятий → аргументы → примеры → вывод.

Дополнительные вопросы:

Преподаватель может углубиться в тему или попросить провести сравнение

Дискуссия (для группового формата):

Студенты высказывают мнения, приводят контраргументы, опираясь на факты.

4. Критерии оценки

Знание материала

Логика изложения

Аргументация (подкрепление тезисов примерами, статистикой).

Культура речи (ясность, отсутствие длинных пауз).

Ответы на вопросы (способность уверенно поддерживать диалог).

5. Рекомендации для студентов

Не заучивайте тексты дословно — говорите своими словами.

Управляйте стрессом: если забыли термин, опишите его.

Тренируйтесь вслух перед зеркалом или с одногруппниками.

6. Важные нюансы

Если вопрос непонятен, можно уточнить у преподавателя.

За некорректное поведение (списывание, подсказки) баллы снижаются.

Результат объявляется сразу или на следующем занятии.

Устный ответ — это возможность показать не только знания, но и умение мыслить критически, поэтому акцент делается на понимание, а не на зазубривание.

Критерии оценивания.

Критерии оценки (дифференцированной):
оценка «отлично» выставляется студенту, если материал изложен грамотно, логически структурирован; работа содержательная и аргументированная; материал подкреплен знанием литературы и источников по теме вопроса; правильно использована юридическая терминология; присутствует четкое изложение дефиниций и классификаций, раскрытие основных признаков и характерных черт понятий, явлений, процессов; содержание работы в полной мере соответствует выбранной теме.
оценка «хорошо» выставляется при наличии незначительного нарушения логики изложения материала, допущено не более двух фактических или терминологических ошибок, присутствует неполнота или неточность в формулировках;
оценка «удовлетворительно» - существенное нарушение логики изложения материала, допущение более двух фактических или терминологических ошибок; содержание работы не в полной мере соответствует выбранной теме.
оценка «неудовлетворительно» - грубое нарушение логики изложения материала,

допущение многочисленных фактических или терминологических ошибок; содержание работы не соответствует выбранной теме.

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-3.2		
ОПК ОС-10.3		
ОПК ОС-3.3		
ОПК ОС-10.2	В ходе текущего контроля успеваемости при ответах на семинарских и практических занятиях обучающиеся оцениваются по четырёхбалльной шкале: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» оценка «отлично» выставляется обучающимся, показавшим всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивших основную и дополнительную литературу, рекомендованную программой. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала; оценка «хорошо» выставляется обучающимся, показавшим полное знание учебно-программного материала, успешно выполняющим предусмотренные в программе задания, усвоившим основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется студентам, продемонстрировавшим	Опрос; Дискуссия; Доклады; Тестирование.

	систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности; оценка «удовлетворительно» выставляется обучающимся, показавшим знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справившимся с выполнением заданий, предусмотренных программой, ориентирующимся в основной литературе, рекомендованной программой. Как правило, оценка «удовлетворительно» выставляется студентам, допустившим погрешности в ответе на занятии и при выполнении заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя; оценка «неудовлетворительно» выставляется обучающимся, имеющим пробелы в знаниях основного учебно-программного материала, допустившим принципиальные ошибки в выполнении предусмотренных программой заданий.	

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 6, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

Процедура проведения экзамена по дисциплине «Защита информации»

Студент получает 1 билета, каждый из которых содержит 1 теоретический вопрос и 1 практическую задачу.

На подготовку отводится 20–30 минут (конкретное время объявляет преподаватель).

Ответ включает:

Развернутое объяснение теории.

Решение практической задачи (например, анализ уязвимости или настройка защиты).

Допускается использование письменных заметок (если разрешено преподавателем).

Оценивается: глубина знаний, точность решения, аргументация.

Дополнительные вопросы задаются только при неполном ответе.

Результат объявляется после завершения ответа.

Пример задания:

Пример билета:

Теория: «Принципы работы межсетевых экранов».

Практика: «Предложите схему защиты сети от DDoS-атак».

Примерный перечень вопросов для экзамена:
Теоретические вопросы
Дайте определение информационной безопасности. Назовите основные принципы (CIA-триада).

Перечислите виды угроз информационной безопасности.

Что такое социальная инженерия? Приведите примеры атак.

Опишите классификацию вредоносного ПО.

В чем разница между симметричным и асимметричным шифрованием?

Объясните принцип работы алгоритма AES.

Для чего используется электронная подпись?

Что такое хеширование? Назовите популярные алгоритмы.

Какие функции выполняет межсетевой экран (firewall)?

Опишите типы VPN и их назначение.

Что такое DDoS-атака и как от нее защититься?

В чем суть атаки «человек посередине» (MITM)?

Назовите методы защиты от фишинга.

Что такое SQL-инъекция и как ее предотвратить?

Объясните принцип работы системы обнаружения вторжений (IDS).

Какие существуют стандарты информационной безопасности (ISO 27001, PCI DSS)?

В чем разница между идентификацией, аутентификацией и авторизацией?

Что такое биометрическая аутентификация? Приведите примеры.

Опишите модель угроз для мобильных устройств.

Какие существуют методы защиты беспроводных сетей (Wi-Fi)?

Практические задачи
Разработайте политику парольной защиты для компании.

Предложите схему защиты локальной сети от внешних атак.

Как настроить VPN для удаленного доступа сотрудников?

Опишите порядок действий при обнаружении вируса в корпоративной сети.

Как проверить, подвержена ли система уязвимости Zero-day?

Рассчитайте надежность пароля по заданным критериям.

Расшифруйте сообщение, закодированное методом Цезаря (сдвиг +3).

Настройте правила файервола для блокировки подозрительного трафика.

Проанализируйте дамп сетевого трафика (Wireshark) на наличие аномалий.

Как защитить веб-приложение от XSS-атак?

Нормативно-правовые аспекты
Какие законы РФ регулируют защиту персональных данных?

В чем суть ФЗ «О критической информационной инфраструктуре»?

Какие санкции предусмотрены за нарушение 152-ФЗ?

Какие данные относятся к коммерческой тайне?

Каковы обязанности администратора ИБ в организации?

Криптография и стеганография
В чем отличие RSA от ECC?

Как работает протокол TLS?

Что такое квантовая криптография?

Опишите принцип стеганографии.

Как защитить данные при передаче через открытые каналы?

Современные угрозы и технологии
Что такое APT-атаки?

Как работает ransomware и как от него защититься?

В чем опасность IoT-устройств для ИБ?

Как блокчейн используется в информационной безопасности?

Какие угрозы несет облачным сервисам?

Дополнительные вопросы
Какие методы защиты применяются в банковской сфере?

Как организовать безопасный удаленный доступ для сотрудников?

Какие существуют международные стандарты ИБ?

Как провести аудит информационной безопасности?

Какие тренды в кибербезопасности будут актуальны в ближайшие 5 лет?

6.2.2.1.2 Критерии оценивания

Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
Полные, развернутые ответы Точное использование терминологии Умение приводить примеры Логичность и последовательность изложения Самостоятельность суждений	В основном полные ответы Незначительные неточности Достаточное владение терминологией Наличие примеров	Ответы на уровне минимальных требований Наличие существенных пробелов Затруднения с примерами	Серьезные пробелы в знаниях Неспособность ответить на основные вопросы Многочисленные ошибки

7 **Основная учебная литература**

1. Краковский, Ю. М. Методы и средства защиты информации : Учебное пособие для вузов / Ю. М. Краковский. – 1-е изд.. – Санкт-Петербург : Издательство ЛАНЬ, 2024. – 272 с. – EDN SWECXC.

8 Дополнительная учебная литература и справочная

1. Ерохин, В. В. Верификация информации и защита программного обеспечения в информационно-телекоммуникационных системах банка / В. В. Ерохин. – 2-е издание, переработанное и дополненное. – Москва : ООО Спутник+, 2025. – 183 с. – ISBN 5-277-01356-3. – EDN MYYDNF.

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 Word

2. Свободно распространяемое программное обеспечение Power Point

12 Материально-техническое обеспечение дисциплины