Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Сибирская школа геонаук (119)»

УТВЕРЖДЕНА:
на заседании ДОТ
Протокол №29 от 10 апреля 2025 г.

Рабочая программа дисциплины

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ / FUNDAMENTALS OF INFORMATION SECURITY»

Направление: 09.03.02 Информационные системы и технологии

Информационные технологии в науках о Земле и окружающей среде / Information Technologies in Earth and Environmental Sciences

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Ланько Анна Викторовна Дата подписания: 19.12.2025	Документ подписан простой электронной подписью Утвердил: Ланько Анна Викторовна Дата подписания: 19.12.2025	Документ подписан простой электронной подписью Согласовал: Паршин Александр Вадимович Дата подписания: 13.01.2026

Год набора – 2025

Иркутск, 2025 г.

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

1.1 Дисциплина «Основы информационной безопасности / Fundamentals of Information Security» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
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-3.7
ОПК ОС-4 Способность участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил	ОПК ОС-4.4

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-3.7	Имеет представление об основных компонентах информационной безопасности и способен применять инструменты обеспечения информационной безопасности в рамках решения задач профессиональной деятельности	**Знать** основные принципы информационной безопасности (конфиденциальность, целостность, доступность), виды угроз, нормативные стандарты и требования, компоненты систем защиты, основы криптографии и методы аутентификации, сетевые протоколы и архитектуры. **Уметь** проводить аудит безопасности систем и сетей, настраивать средства защиты данных, анализировать сетевой трафик, выявлять угрозы безопасности, применять методы шифрования, документировать и реагировать на инциденты безопасности. **Владеть** инструментами анализа сетевого трафика, сканирования сетей и поиска уязвимостей, генерации криптографических ключей и шифрования, тестирования на проникновение, комплексными средами для обеспечения безопасности, настройкой правил файрволов.
ОПК ОС-4.4	Способен составлять рабочую	**Знать** требования стандартов к

	документацию в соответствии с требованиями стандартов по обеспечению информационной безопасности	документации по информационной безопасности, структуру политик безопасности, регламенты реагирования на инциденты, шаблоны отчетов об аудитах, форматы описания процедур и инструкций. **Уметь** разрабатывать политики безопасности организации, составлять инструкции по защите данных, оформлять отчеты о выявленных уязвимостях, описывать процедуры реагирования на инциденты, вести журналы событий безопасности. **Владеть** шаблонами документов по стандартам информационной безопасности, текстовыми редакторами для оформления регламентов, системами управления документацией, средствами автоматизации отчетности по безопасности.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Основы информационной безопасности / Fundamentals of Information Security» базируется на результатах освоения следующих дисциплин/практик: «Геоинформационные технологии / Geoinformation Technologies», «Архитектура информационных систем / Information System Architecture», «Базы данных / Databases»

Дисциплина является предшествующей для дисциплин/практик: «Проектирование информационных систем / Information Systems Design», «Надежность информационных систем / Reliability of Information Systems»

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 № 5
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	45	45
лекции	15	15
лабораторные работы	30	30
практические/семинарские занятия	0	0
Самостоятельная работа (в т.ч. курсовое проектирование)	63	63
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 № 5

№ 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	1. Основы информационной безопасности	1	2	1	2			3	8	Устный опрос
2	2. Криптографические методы защиты данных	2	2	2, 3	8			1	10	Устный опрос
3	3. Сетевая безопасность и анализ трафика	3	2	4	4			3	15	Устный опрос
4	4. Аудит безопасности и сканирование уязвимостей	4	3	5, 6	8			4	10	Устный опрос
5	5. Средства защиты сетей	5	2	7	4			5	10	Устный опрос
6	6. Тестирование на проникновение и документация	6	4	8	4			2	10	Устный опрос
	Промежуточная аттестация									Зачет с оценкой
	Всего		15		30				63	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 5

№	Тема	Краткое содержание
1	1. Основы информационной безопасности	Принципы конфиденциальности, целостности и доступности информации, классификация угроз безопасности, модель оценки рисков и ущерба, нормативные требования к защите информации.
2	2. Криптографические методы защиты данных	Симметричное и асимметричное шифрование данных, хэш-функции для проверки целостности, цифровые подписи и сертификаты, инфраструктура открытых ключей.
3	3. Сетевая безопасность и анализ трафика	Протоколы сетевого взаимодействия, этапы установления соединений,
4	4. Аудит безопасности и сканирование уязвимостей	Методы сканирования сетей, обнаружение операционных систем и сервисов, базы данных уязвимостей, автоматизированные средства

		аудита.
5	5. Средства защиты сетей	Файрволы и системы фильтрации пакетов, трансляция сетевых адресов, виртуальные частные сети, зоны безопасности, логирование событий.
6	6. Тестирование на проникновение и документация	Этапы тестирования на проникновение, средства эксплуатации уязвимостей, составление отчетов по безопасности, разработка политик и регламентов.

4.3 Перечень лабораторных работ

Семестр № 5

№	Наименование лабораторной работы	Кол-во академических часов
1	Лабораторная работа №1. Классификация угроз информационной безопасности	2
2	Лабораторная работа №2. Шифрование файлов симметричными алгоритмами	4
3	Лабораторная работа №3. Генерация ключей и цифровые подписи	4
4	Лабораторная работа №4. Захват и анализ сетевого трафика	4
5	Лабораторная работа №5. Сканирование сети	4
6	Лабораторная работа №6. Анализ уязвимостей	4
7	Лабораторная работа №7. Настройка файрволов	4
8	Лабораторная работа №8. Базовый пентест	4

4.4 Перечень практических занятий

Практических занятий не предусмотрено

4.5 Самостоятельная работа

Семестр № 5

№	Вид СРС	Кол-во академических часов
1	Оформление отчетов по лабораторным и практическим работам	10
2	Подготовка к зачёту	10
3	Подготовка к практическим занятиям (лабораторным работам)	23
4	Подготовка к сдаче и защите отчетов	10
5	Проработка разделов теоретического материала	10

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: работа в малых группах

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по лабораторным работам:

Лабораторная работа №1. Классификация угроз информационной безопасности
Цель: Изучить принципы безопасности и классифицировать угрозы по нарушению конфиденциальности, целостности и доступности.
Ход выполнения работы:
1. Открыть LibreOffice Calc и создать таблицу с колонками "Угроза", "Принцип CIA", "Пример", "Ущерб".
2. В браузере найти 10 реальных кейсов инцидентов (Equifax, WannaCry, SolarWinds).
3. Заполнить таблицу, классифицируя угрозы по принципам безопасности.
4. В Draw.io построить матрицу рисков (ось X — вероятность, ось Y — ущерб, цветовая маркировка).
5. Сохранить отчет в формате PDF.

Ожидаемые результаты:
Таблица классификации, матрица рисков с цветовой маркировкой.
Контрольные вопросы:
1. Какая угроза нарушает доступность?
2. Пример нарушения целостности?

Лабораторная работа №2. Шифрование файлов симметричными алгоритмами
Цель: Освоить симметричное шифрование файлов и сравнить режимы работы алгоритмов.
Ход выполнения работы:
1. Создать тестовый файл text.txt (1 МБ случайного текста).
2. Выполнить шифрование в режиме ECB: команда с паролем.
3. Повторить для режимов CBC и GCM с замерами времени.
4. Расшифровать все файлы и проверить целостность.
5. Составить таблицу сравнения режимов.

Ожидаемые результаты:
Зашифрованные файлы, таблица сравнения по времени и размеру.
Контрольные вопросы:
1. Почему ECB-режим небезопасен?
2. Роль вектора инициализации?

Лабораторная работа №3. Генерация ключей и цифровые подписи
Цель: Научиться создавать криптографические ключи и проверять цифровые подписи.
Ход выполнения работы:
1. Сгенерировать пару ключей с именем "Student".
2. Экспортировать публичный ключ в файл.
3. Подписать тестовый файл.
4. Проверить подпись на оригинальном файле.
5. Импортировать ключ и проверить подпись на другой машине.

Ожидаемые результаты:
Файлы ключей и подписи, отчет верификации.
Контрольные вопросы:
1. Разница между шифрованием и подписью?
2. Можно ли подделать подпись?

Лабораторная работа №4. Захват и анализ сетевого трафика
Цель: Освоить анализ сетевого трафика и выявление подозрительной активности.
Ход выполнения работы:
1. Запустить анализатор трафика и выбрать сетевой интерфейс.
2. Сгенерировать тестовый трафик (HTTP, ping).
3. Применить фильтры для поиска паролей и SYN-пакетов.

4. Построить графики IO и статистику протоколов.
5. Экспортировать отчет анализа.

Ожидаемые результаты:

Отчет с примерами аномалий, диаграмма протоколов.

Контрольные вопросы:

1. Что показывает большое количество SYN?
2. Фильтр для HTTP трафика?

Лабораторная работа №5. Сканирование сети

Цель: Научиться обнаруживать хосты, сервисы и операционные системы в сети.

Ход выполнения работы:

1. Выполнить обнаружение хостов в подсети.
2. Просканировать 100 наиболее популярных портов.
3. Провести полное сканирование с определением версий и ОС.
4. Запустить скриптовое сканирование уязвимостей.
5. Сохранить отчет в XML и конвертировать в HTML.

Ожидаемые результаты:

Отчет с топ-10 портов, таблица обнаруженных сервисов.

Контрольные вопросы:

1. Разница SYN и TCP Connect сканирования?
2. Зачем version detection?

Лабораторная работа №6. Анализ уязвимостей

Цель: Провести автоматизированный анализ уязвимостей системы.

Ход выполнения работы:

1. Создать цель сканирования (IP уязвимой машины).
2. Настроить конфигурацию сканирования и запустить задачу.
3. После завершения открыть отчет и отсортировать по степени опасности.
4. Выделить 5 наиболее критических уязвимостей.
5. Экспортировать отчет в HTML/PDF.

Ожидаемые результаты:

Отчет с топ-5 уязвимостями, план их устранения.

Контрольные вопросы:

1. Что означает высокий балл опасности 9.8?
2. Разница уязвимости и эксплойта?

Лабораторная работа №7. Настройка файрволов

Цель: Настроить правила файрвола для защиты системы от несанкционированного доступа.

Ход выполнения работы:

1. Сохранить текущие правила файрвола.
2. Установить политику по умолчанию "запретить все".
3. Разрешить доступ по портам SSH, HTTP, HTTPS.
4. Настроить трансляцию сетевых адресов.
5. Протестировать правила сканированием и сохранить конфигурацию.

Ожидаемые результаты:

Файл правил файрвола, отчет сканирования до/после.

Контрольные вопросы:

1. Разница между блокировкой и отклонением пакетов?
2. Зачем нужна политика "запретить все"?

Лабораторная работа №8. Базовый пентест
Цель: Провести контролируемое тестирование на проникновение с составлением отчета.
Ход выполнения работы:
1. Запустить консоль тестирования на проникновение.
2. Найти эксплойт для известной уязвимости.
3. Настроить параметры атаки (цель, локальный хост).
4. Запустить эксплойт и получить удаленный доступ.
5. Выполнить команды диагностики системы и сделать скриншоты.
6. Составить отчет с рекомендациями.
Ожидаемые результаты:
Скриншоты сессии доступа, отчет пентеста.
Контрольные вопросы:
1. Основные этапы тестирования на проникновение?
2. Что такое полезная нагрузка эксплойта?

5.1.2 Методические указания для обучающихся по самостоятельной работе:

Рекомендации по самостоятельной работе:
1. Рекомендации по самостоятельной подготовке к лабораторным работам
• Изучите теоретический материал по теме лабораторной работы. Ознакомьтесь с учебниками, лекциями и дополнительными источниками, чтобы понимать цели и задачи работы, основные понятия и методы, используемые в лабораторном задании1.
• Внимательно ознакомьтесь с методическими указаниями и требованиями к лабораторной работе. Обратите внимание на последовательность выполнения этапов, используемое программное обеспечение, форматы исходных и выходных данных, требования к визуализации и анализу результатов.
• Подготовьте исходные данные. Проверьте наличие всех необходимых файлов, убедитесь в их корректности (форматы, структура, отсутствие ошибок и пропусков данных).
• Освойте необходимые функции и инструменты программного обеспечения. Повторите работу с теми модулями и инструментами, которые будут использоваться в лабораторной работе.
• Планируйте время. Разделите выполнение работы на этапы: подготовка данных, выполнение анализа, оформление визуализации, написание отчета.
2. Рекомендации по оформлению отчетов по лабораторным работам
• Структурируйте отчет по стандартной схеме:
• Титульный лист (название работы, ФИО, группа, дата)
• Цель работы
• Краткое описание исходных данных
• Описание используемых методов и программного обеспечения
• Последовательное изложение этапов работы с иллюстрациями (скриншотами, графиками, картами)
• Анализ полученных результатов (выявленные особенности, сравнение с теорией, интерпретация)
• Выводы и рекомендации
• Список использованных источников
• Используйте качественные иллюстрации. Все графические материалы должны быть четкими, снабжены подписями, масштабами, легендами и пояснениями.
• Формулируйте выводы по существу. Кратко и ясно отражайте основные

результаты работы, выявленные закономерности, достоинства и ограничения применяемых методов.

- Оформляйте отчет в соответствии с требованиями ДОТ. Соблюдайте стандарты оформления текста, таблиц, рисунков и ссылок на источники.

3. Рекомендации по самостоятельной проработке отдельных разделов тем

- Изучайте рекомендованную литературу и дополнительные источники. Используйте учебники, статьи, электронные ресурсы, профессиональные базы данных и справочные материалы, указанные в рабочей программе дисциплины1.
- Выполняйте конспектирование ключевых понятий и алгоритмов. Составляйте краткие записи по основным определениям, алгоритмам, этапам работы с ПО, особенностям визуализации и анализа данных.
- Практикуйтесь в самостоятельном выполнении типовых заданий. Решайте задачи, связанные с обработкой и визуализацией геолого-геофизических данных, используя различные программные средства.
- Формулируйте вопросы и уточнения для обсуждения на занятиях. Записывайте непонятные моменты, чтобы получить разъяснения у преподавателя или в ходе дискуссии.
- Анализируйте примеры из практики. Изучайте реальные кейсы решения задач геофизики, сравнивайте разные подходы и делайте выводы о целесообразности их применения.

4. Общие рекомендации

- Развивайте навыки поиска и критического анализа информации. Пользуйтесь современными информационными ресурсами, анализируйте достоверность и актуальность найденных данных.
- Акцентируйте внимание на интеграции знаний и умений. Старайтесь связывать теоретические знания с практическими задачами, анализируйте, как выбранные методы и технологии влияют на качество и достоверность графического представления информации.
- Соблюдайте академическую честность. Все результаты, представленные в отчетах, должны быть получены самостоятельно, с обязательным указанием источников заимствованных данных и иллюстраций.

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 5 | Устный опрос

Описание процедуры.

Опрос может проводиться:
Фронтально — в форме беседы с группой, когда вопросы задаются всей группе, а ответы даются по очереди или по желанию.
Индивидуально — каждый студент отвечает на один или несколько вопросов, давая развернутый, связный ответ, часто с примерами и пояснениями.
Комбинированно — сочетаются оба подхода, а также используются дополнительные методы (например, письменные карточки, рецензирование ответов товарищей)

Критерии оценивания.

полнота и правильность ответа;
понимание и осознанность материала;
логичность и последовательность изложения;
корректность терминологии;
способность отвечать на уточняющие вопросы

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-3.7	Критерии оценивания полнота и правильность ответа; понимание и осознанность материала; логичность и последовательность изложения; корректность терминологии; способность отвечать на уточняющие вопросы	устный опрос
ОПК ОС-4.4	Критерии оценивания полнота и правильность ответа; понимание и осознанность материала; логичность и последовательность изложения; корректность терминологии; способность отвечать на уточняющие вопросы	устный опрос

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 5, Типовые оценочные средства для проведения дифференцированного зачета по дисциплине

6.2.2.1.1 Описание процедуры

К зачету допускаются студенты сдавшие все отчеты по лабораторным (практическим) работам. Зачёт проводится в форме устного опроса или тестирования, включающего 5 вопросов — по одному из каждой основной темы курса. В некоторых случаях допускается комбинированная форма: тест + устный опрос.
Время на ответ ограничено, ответы должны быть чёткими, логичными и аргументированными.
В случае неудовлетворительного результата студенту предоставляется возможность пересдачи в установленные сроки. При повторном не сдаче возможна дополнительная консультация и индивидуальное собеседование. Оценка выставляется по шкале с учётом полноты и правильности ответов.

6.2.2.1.2 Критерии оценивания

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Ответ полный, логичный и структурированный, раскрывает все теоретические вопросы билета. Приведены корректные определения, пояснения, примеры и ссылки на нормативные документы (при необходимости). Практическое задание выполнено полностью, расчеты верны, использованы правильные методы и обоснования. Ответ демонстрирует глубокое понимание материала, самостоятельность мышления и умение применять знания на практике.	Ответ в целом полный, но есть незначительные неточности или упущены отдельные детали. Теоретические вопросы раскрыты, приведены основные определения и примеры. Практическое задание выполнено правильно, но возможны несущественные ошибки или недостаточно подробные пояснения. Понимание материала хорошее, умение применять знания продемонстрировано.	Ответ частичный, раскрывает основные положения, но есть существенные пробелы или ошибки в теории. Некоторые определения отсутствуют или даны неверно, примеры не приведены либо не соответствуют вопросу. Практическое задание выполнено частично, есть ошибки в расчетах или не все этапы решения отражены. Понимание материала поверхностное, самостоятельность ограничена.	Ответ не раскрывает основные вопросы билета, содержит грубые ошибки или существенные пробелы. Теоретические положения изложены неверно или отсутствуют. Практическое задание не выполнено либо выполнено неправильно, расчеты отсутствуют или неверны. Материал не усвоен, самостоятельность отсутствует.

7 Основная учебная литература

1. Мельников, А. В. Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва : РГУП, 2025. — 220 с. — ISBN 978-5-00209-188-1. — Текст : электронный // Лань : электронно-библиотечная система.

2. Рейн, Т. С. Основы информационной безопасности : учебное пособие / Т. С. Рейн, В. В. Торгулькин. — Кемерово : КемГУ, 2024. — 117 с. — ISBN 978-5-8353-3270-0. — Текст : электронный // Лань : электронно-библиотечная система.

8 Дополнительная учебная литература и справочная

1. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 324 с. — ISBN 978-5-507-49077-6. — Текст : электронный // Лань : электронно-библиотечная система.

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.