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 №9 от 27 февраля 2025 г.

Рабочая программа дисциплины

«ЗАЩИТА ИНФОРМАЦИИ»

Направление: 09.03.01 Информатика и вычислительная техника

Вычислительные машины, комплексы, системы и сети

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Аношко Алексей Федорович Дата подписания: 26.08.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 27.08.2025	Документ подписан простой электронной подписью Согласовал: Аношко Алексей Федорович Дата подписания: 08.08.2025

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» 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-10.2
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-3.3
ОПК ОС-6 Способность разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием	ОПК ОС-6.4

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-10.2	Способность осваивать и использовать программное обеспечение для решения практических задач информационной безопасности и защиты информации	**Знать** Классификацию и назначение ПО ИБ Принципы работы ключевых категорий ПО Модели угроз Основные требования стандартов и регуляторов Потенциальные риски и ограничения ПО ИБ **Уметь** Выполнять инсталляцию, базовую и тонкую настройку различных типов ПО ИБ под конкретные задачи и инфраструктуру. Сопровождать ПО ИБ. Диагностировать и устранять базовые неисправности в работе ПО ИБ; понимать сообщения об ошибках **Владеть** Навыками использования ПО ИБ Навыками автоматизации рутинных задач Навыками документирования
ОПК ОС-3.3	Способность использовать информационно-коммуникационные технологии,	**Знать** Основные операции и преобразования: детерминизация, минимизация, проверка

	информационную и библиографическую культуру с учетом требований информационной безопасности для решения практических задач теории автоматов	эквивалентности. Возможности и ограничения конкретных инструментов Роль автоматов в ИБ: моделирование протоколов аутентификации, анализа сетевого трафика (IDS/IPS), детектирование вредоносного ПО, синтез защищенных схем. **Уметь** Определять, содержит ли решаемая задача или используемая модель конфиденциальную информацию. Разбирать ошибки в моделях автоматов могут привести к уязвимостям безопасности. **Владеть** Уверенное владение интерфейсом и функционалом 1-2 специализированных программ для моделирования и анализа автоматов (например, JFLAP, конкретная библиотека на Python/C++).
ОПК ОС-6.4	Разработка планов и технического задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием с учетом информационной безопасности	**Знать** Основы проектирования ИТ-инфраструктуры **Уметь** Формировать архитектурные решения и ТЗ по построению/модернизации ИТ-инфраструктуры с учетом требований ИБ **Владеть** Методологией проектирования защищенной ИТ-инфраструктуры

2 Место дисциплины в структуре ООП

Изучение дисциплины «Защита информации» базируется на результатах освоения следующих дисциплин/практик: «Введение в профессиональную деятельность», «Дискретная математика», «Теория автоматов», «Операционные системы»

Дисциплина является предшествующей для дисциплин/практик: «Основы ИТ-менеджмента», «Безопасность Linux систем», «Проектирование информационных систем»

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:	64	64
лекции	32	32

лабораторные работы	32	32
практические/семинарские занятия	0	0
Самостоятельная работа (в т.ч. курсовое проектирование)	44	44
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	2					3	32	Отчет по лабораторной работе
2	PKI и электронная подпись	8	2	5	4			2	8	Отчет по лабораторной работе
3	Анализ электронных журналов	7	2	6	8					Отчет по лабораторной работе
4	Антивирусные системы	3	2	4	4					Отчет по лабораторной работе
5	Аппаратные угрозы	2	4							Отчет по лабораторной работе
6	Межсетевые экраны	5	2	3	4					Отчет по лабораторной работе
7	Отказоустойчивость систем	6	2	2	4					Отчет по лабораторной работе
8	Сетевая безопасность	11	4							Отчет по лабораторной работе
9	Системы обнаружения вторжений	4	4					1	4	Отчет по лабораторной работе
10	Социальная инженерия	9	2							Отчет по лабораторной работе
11	Стандарты ИБ	10	6	1	8					Отчет по лабораторной работе
	Промежуточная аттестация								36	Экзамен
	Всего		32		32				80	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 6

№	Тема	Краткое содержание
1	Введение в информационную безопасность	Основные принципы (конфиденциальность, целостность, доступность), угрозы для технических систем, нормативная база ФСТЭК
2	PKI и электронная подпись	Структура PKI. Процесс создания и использования электронной подписи Законодательное регулирование
3	Анализ электронных журналов	Источники данных для анализа Инструменты анализа: Open-source инструменты: Logstash, Elasticsearch, Graylog. Коммерческие продукты: Splunk, IBM QRadar, SolarWinds LEM. Типичные сценарии использования
4	Антивирусные системы	Принцип работы антивирусных систем. Современные типы антивирусных решений Эффективность и ограничения антивирусных систем
5	Аппаратные угрозы	Классификация аппаратных угроз. Примеры аппаратных угроз Методы защиты от аппаратных угроз
6	Межсетевые экраны	Функции межсетевых экранов. Типы межсетевых экранов. Рекомендации по выбору и настройке межсетевых экранов
7	Отказоустойчивость систем	Причины сбоев и отказов. MTBF (Mean Time Between Failures) — среднее время между отказами, и параметром MTTR (Mean Time To Repair) — среднее время восстановления работоспособности. Методы и примеры решений достижения отказоустойчивости
8	Сетевая безопасность	Уровни сетевой безопасности. Типичные угрозы сетевой безопасности Средства защиты сети Облачная безопасность (Cloud Security): Особенности защиты данных и приложений в IaaS, PaaS, SaaS моделях.
9	Системы обнаружения вторжений	Типы систем обнаружения вторжений. Способы обнаружения вторжений. Этапы работы и примеры систем обнаружения вторжений (IDS)
10	Социальная инженерия	Методы манипуляции (фишинг, претекстинг, кви про кво), принципы создания культуры безопасности (security awareness training) и политики работы с персоналом.
11	Стандарты ИБ	Требования ФСТЭК/ФСБ к вычислительным комплексам и телекоммуникационным системам,

		сертификация СЗИ.152-ФЗ в РФ, GDPR

4.3 Перечень лабораторных работ

Семестр № 6

№	Наименование лабораторной работы	Кол-во академических часов
1	Анализ рисков ИБ на примере реальной организации и разработка политики безопасности.	8
2	Исследование аппаратных уязвимостей (Spectre/Meltdown) и конфигурация базовой отказоустойчивости.	4
3	Настройка и тестирование сетевого экрана (iptables/nftable)	4
4	Сравнительный анализ эффективности антивирусных продуктов.	4
5	Создание корневой инфраструктуры PKI и выпуск сертификатов. Подпись и проверка документов.	4
6	Централизованный сбор и анализ журналов событий с помощью ELK Stack (Elasticsearch, Logstash, Kibana).	8

4.4 Перечень практических занятий

Практических занятий не предусмотрено

4.5 Самостоятельная работа

Семестр № 6

№	Вид СРС	Кол-во академических часов
1	Выполнение компьютерных экспериментов и компьютерных лабораторных работ в дистанционном режиме	4
2	Подготовка к зачёту	8
3	Подготовка к практическим занятиям	32

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

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:

1)
Задачи:
Описать вымышленную организацию.

Использовать OWASP Risk Assessment Framework или шаблоны из Mozilla Information Security (MIG) для идентификации угроз (включая социальную инженерию) и уязвимостей.
Оценить риски с помощью простой матрицы (вероятность/влияние).
Использовать Open-Source шаблоны политик (например, от SANS Institute или из репозиториев GitHub) для разработки фрагмента политики (напр., "Политика парольной аутентификации" или "Политика обработки ПДн").
Сопоставить меры защиты с требованиями ISO/IEC 27001 (текст стандарта доступен для ознакомления) или NIST SP 800-53 (Open).
Инструменты: OWASP Risk Assessment Methodology, Mozilla MIG шаблоны, SANS Policy Templates (Open-Source версии), тексты ISO 27001/NIST SP 800-53.

2)
Задачи:
Установить Альт Линукс в виртуальной среде.
Использовать spectre-meltdown-checker (Linux) для проверки системы на уязвимости Spectre/Meltdown.
Проанализировать вывод, найти информацию о примененных мерах защиты (микрокод, ядро).
Настроить программный RAID 1 (зеркало) с помощью mdadm (Linux) или LVM Mirroring на виртуальных дисках.
Сымитировать отказ диска (mdadm --set-faulty или физическое отключение диска в VM).
Проверить работоспособность системы и восстановление массива.
Проанализировать журналы (journalctl, /var/log/syslog).
Инструменты: spectre-meltdown-checker, mdadm, LVM (Linux), journalctl, grep.
3)
Использовать виртуальную операционную систему из второй лабораторной работы.
Настроить nftables (или iptables) на сервере:
Разрешить только SSH (tcp/22), HTTP (tcp/80), HTTPS (tcp/443).
Запретить все входящие соединения по умолчанию.
Заблокировать ICMP-запросы (опционально).
Разрешить доступ к веб-серверу только с IP клиента.
С Attacker использовать nmap, hping3 для тестирования правил:
Сканирование портов (-sS, -sV).
Проверка доступности сервисов (telnet, nc).
Проверка блокировки ICMP (ping).
С Client проверить доступ к разрешенным сервисам.
Инструменты: VirtualBox/Proxmox/GNS3, Linux (Debian/Ubuntu), nftables/iptables, nmap, hping3, telnet/netcat.
4)Провести аналитику обзоров существующих любых трех антивирусных систем.
Составить рейтинговую таблицу с их описанием.
5)Задачи:
Создать корневой УЦ (CA) с помощью OpenSSL:
Генерация приватного ключа и самоподписанного сертификата.
Создать и подписать сертификат сервера (для веб-сервера Apache/Nginx).
Создать и подписать сертификат пользователя.
Настроить веб-сервер Apache или Nginx на использование HTTPS с созданным сертификатом.
Установить корневой сертификат УЦ в хранилище клиента (браузер или ОС).
Подписать текстовый файл с помощью GnuPG (GPG) или создать и подписать PDF с помощью LibreOffice или OpenSSL (smime).

Проверить подпись документа. Проверить файл, подписанный другим УЦ (другого студента)
Инструменты: OpenSSL, Apache/Nginx, GPG (GnuPG), LibreOffice, браузер (Firefox/Chrome).
6)Задачи:
Развернуть Elasticsearch, Logstash, Kibana (использовать Open Distro for Elasticsearch или чистый OSS версии).
Установить и настроить Filebeat на Linux-клиенте для сбора системных логов (syslog, auth.log).
Установить и настроить Winlogbeat на Windows-клиенте (опционально, если есть Windows ВМ) для сбора Event Logs.
Настроить Logstash для приема логов от Beats и их парсинга (фильтры grok).
Создать индексы в Elasticsearch.
В Kibana:
Создать Index Patterns.
Построить визуализации: график неудачных логинов, таблица пользователей с ошибками ввода пароля, карта источников атак.
Создать дашборд из визуализаций.
Сгенерировать события неудачных логинов и отследить их в Kibana.
Инструменты: Elasticsearch OSS, Logstash OSS, Kibana OSS, Filebeat, Winlogbeat, Linux

5.1.2 Методические указания для обучающихся по самостоятельной работе:

- Подготовка к лабораторным занятиям.
Цель: работа с методическими указаниями к выполнению работы, конспектом лекций, дополнительными источниками информации, повторение материла для защиты работы.
- Проработка отдельных разделов теоретического курса.
Цель: получение более глубоких знаний и навыков по специальным разделам дисциплины

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 | Отчет по лабораторной работе

Описание процедуры.

Защита лабораторной работы проводится в форме устного опроса обучающегося. Вопросы касаются защищаемой работы. При этом, кроме теоретической составляющей, при защите работы преподаватель может попросить продемонстрировать навыки работы с ПО, умение проектировать базу данных на небольших задачах.

Критерии оценивания.

Работа считается защищенной при выполнении всех требований к ее выполнению и оформлению, а также правильных ответах при ее защите, умении продемонстрировать на небольших задачах навыки, которым посвящена лабораторная работа.

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-10.2	Способен осваивать и использовать программное обеспечение для решения практических задач информационной безопасности и защиты информации	Устное собеседование и/или практические задания
ОПК ОС-3.3	Способен осваивать и использовать программное обеспечение для решения практических задач информационной безопасности и защиты информации	Устное собеседование и/или практические задания
ОПК ОС-6.4	Разрабатывает планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием с учетом информационной безопасности	Устное собеседование и/или практические задания

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

Экзамен проводиться в форме устного опроса по билетам (вопросам), с предварительной подготовкой. К каждому билету прилагается практическая задача по темам лабораторных работ

Пример задания:

Билет №4
Руководящие документы Гостехкомиссии
Перечислите показатели защищенности СВТ от НСД. Как классифицируются автоматизированные системы по уровню защищенности?

Электронная подпись и нормативная база
Назовите законодательные акты, регулирующие применение ЭП в РФ. Как процедура формирования ЭП обеспечивает юридическую значимость?

Практика
Составьте схему использования ЭП в документообороте госучреждения с учетом требований ФЗ № 63 "Об ЭП".

6.2.2.1.2 Критерии оценивания

Отлично	Хорошо	Удовлетворительн	Неудовлетворительно

		о	
Наличие глубоких знаний в объеме пройденного программного материала, правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы.	достаточно полное понимание предмета, хорошие знания, умения и владения	достаточно полное понимание предмета, хорошие знания, умения и владения	результаты обучения не соответствуют минимальным требованиям. Не владеет основными понятиями и не может применить знания в решении задач.

7 Основная учебная литература

1. Кибербезопасность. Главные принципы (pdf+epub).320 стр. 2023г.

2. Никита Скрамцов, Kali Linux в действии. Аудит безопасности информационных систем (pdf+epub).
Дата написания: 2024
Объем: 385 стр.
ISBN: 978-5-4461-2154-0

8 Дополнительная учебная литература и справочная

1. Цифровая гигиена, авторы: Игорь Ашманов, Наталья Касперская
Дата написания: 2022
Объем: 508 стр. 97 иллюстраций
ISBN: 978-5-4461-1938-7

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.