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

«МОНИТОРИНГ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»

Направление: 09.03.02 Информационные системы и технологии

Информационные системы и технологии в административном управлении

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Аршинский Вадим Леонидович Дата подписания: 19.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 19.06.2025	Документ подписан простой электронной подписью Согласовал: Аршинский Вадим Леонидович Дата подписания: 19.06.2025

Год набора – 2025

Иркутск, 2025 г.

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

1.1 Дисциплина «Мониторинг безопасности информационных систем» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ПКС-3 Способен обеспечивать эффективную работу баз данных, являющихся частью различных информационных систем, включая развертывание, сопровождение, оптимизацию их функционирования	ПКС-3.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПКС-3.2	Способен осуществлять сбор и исследование сведений информационной безопасности при администрировании информационных систем и применять системы мониторинга информационной безопасности	**Знать** основные виды угроз информационной безопасности информационных систем. **Уметь** обнаруживать возможные атаки и уязвимости информационных систем. **Владеть** применять технологии сбора и анализа сведений для обнаружения возможных атак и уязвимостей информационных систем.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Мониторинг безопасности информационных систем» базируется на результатах освоения следующих дисциплин/практик: «Основы информационной безопасности», «Web-программирование», «Инфокоммуникационные системы и сети», «Базы данных»

Дисциплина является предшествующей для дисциплин/практик: «Производственная практика: преддипломная практика»

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 № 7
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	48	48
лекции	16	16
лабораторные работы	32	32
практические/семинарские занятия	0	0
Самостоятельная работа (в т.ч. курсовое проектирование)	60	60

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 № 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	Анализ сетевого трафика для обнаружения аномалий и потенциальных угроз	1	2	1	4			1, 1	16	Устный опрос
2	Использование инструментов для мониторинга и анализа журналов для выявления аномальной активности	2	2	2	4			1	8	Устный опрос
3	Использование системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) для обнаружения и блокирования атак	3	2	3	4			1	8	Устный опрос
4	Методы сканирования и анализа приложений на наличие уязвимостей	4	2	4	4					Устный опрос
5	Сбор и анализ данных о безопасности операционных систем	5	2	5	4			1	7	Устный опрос
6	Методы анализа угроз на уровне приложений	6	2	6	4			1	7	Устный опрос
7	Использование инструментов для анализа угроз на основе поведения	7	2	7	4			1	7	Устный опрос
8	Применение	8	2	8	4			1	7	Устный

	машинного обучения в области анализа угроз									опрос
	Промежуточная аттестация									Зачет с оценкой
	Всего		16		32				60	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 7

№	Тема	Краткое содержание
1	Анализ сетевого трафика для обнаружения аномалий и потенциальных угроз	Эта тема охватывает основные принципы и методы анализа сетевого трафика с целью обнаружения аномалий и потенциальных угроз. Включает в себя изучение типов атак, методов защиты сети, инструментов для мониторинга трафика и выявления угроз.
2	Использование инструментов для мониторинга и анализа журналов для выявления аномальной активности	Здесь рассматривается использование специализированных инструментов для сбора, мониторинга и анализа журналов событий с целью выявления аномальной активности, а также для отслеживания действий пользователей и системы
3	Использование системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) для обнаружения и блокирования атак	Эта тема фокусируется на системах обнаружения вторжений (IDS) и предотвращения вторжений (IPS), которые используются для обнаружения и блокирования атак на сеть или систему. Рассматриваются принципы работы, типы атак, возможности конфигурации и эффективность защиты.
4	Методы сканирования и анализа приложений на наличие уязвимостей	Здесь изучается процесс сканирования и анализа приложений на наличие уязвимостей, которые могут быть использованы злоумышленниками для атаки на систему. Эта тема в себя методы тестирования безопасности приложений и применение специализированных инструментов
5	Сбор и анализ данных о безопасности операционных систем	Эта тема описывает использование инструментов для мониторинга безопасности операционных систем, включая сбор данных о событиях, угрозах и уязвимостях. Рассматриваются методы обнаружения аномалий и реагирования на потенциальные угрозы.
6	Методы анализа угроз на уровне приложений	Здесь рассматриваются инструменты и техники для выявления угроз, связанных с приложениями. Эта тема включает в себя методы аудита приложений, сканирования кода на наличие уязвимостей и мониторинг безопасности приложений в реальном времени.
7	Использование инструментов для	Эта тема описывает технологии, позволяющие выявлять аномальное поведение пользователей и

	анализа угроз на основе поведения	системы, что может свидетельствовать о возможных угрозах. Здесь рассматриваются методы машинного обучения, статистического анализа и другие подходы.
8	Применение машинного обучения в области анализа угроз	В этой теме изучается использование методов машинного обучения для обработки больших объемов данных, выявления паттернов и предсказания потенциальных угроз в кибербезопасности. Рассматриваются различные подходы к применению машинного обучения в области обнаружения и предотвращения кибератак.

4.3 Перечень лабораторных работ

Семестр № 7

№	Наименование лабораторной работы	Кол-во академических часов
1	Анализ сетевого трафика для обнаружения аномалий и угроз	4
2	Исследование методов сбора и анализа журналов с использованием специализированных инструментов	4
3	Настройка и тестирование систем IDS и IPS для обнаружения и предотвращения атак	4
4	Анализ уязвимостей приложений с использованием инструментов сканирования и анализа	4
5	Сбор и анализ данных о безопасности операционных систем с применением специализированных средств мониторинга	4
6	Анализ угроз на уровне приложений	4
7	Исследование инструментов для анализа угроз на основе поведения и практическое их применение	4
8	Использование ML для анализа угроз	4

4.4 Перечень практических занятий

Практических занятий не предусмотрено

4.5 Самостоятельная работа

Семестр № 7

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям (лабораторным работам)	60

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 лабораторным работам:

В процессе лабораторного занятия студенты выполняют одну или несколько лабораторных работ (заданий) под руководством преподавателя в соответствии с изучаемым содержанием учебного материала.
Выполнение студентами лабораторных работ направлено на: обобщение, систематизацию, углубление теоретических знаний по конкретным темам учебной дисциплины; формирование умений применять полученные знания в практической деятельности, формирование компетенций; развитие аналитических, проектировочных, конструктивных умений; выработку самостоятельности, ответственности и творческой инициативы.
Лабораторные занятия как вид учебной деятельности должны проводиться в специально оборудованных лабораториях, где выполняются лабораторные работы (задания).
Необходимые структурные элементы лабораторного занятия: инструктаж, проводимый преподавателем; самостоятельная деятельность студентов; обсуждение итогов выполнения лабораторной работы (задания).

5.1.2 Методические указания для обучающихся по самостоятельной работе:

Самостоятельная работа - это основа полноценного образования, планируемая и выполняемая работа обучающихся по заданию, и при методическом руководстве преподавателя, но без его непосредственного участия. Цель самостоятельной работы - научить обучающегося осмысленно и самостоятельно работать с учебным материалом, с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение и стремление в дальнейшем непрерывно повышать свою квалификацию.
Самостоятельная работа выполняет ряд важных функций: развивающая (повышение культуры умственного труда, обогащение интеллектуальных способностей обучающихся); ориентирующая и стимулирующая (процессу обучения придается ускорение и мотивация); воспитательная (формируются и развиваются профессиональные качества специалиста); исследовательская (новый уровень профессионально-творческого мышления); информационно-обучающая (учебная деятельность обучающихся на аудиторных занятиях).
Задачи самостоятельной работы: систематизация и закрепление полученных теоретических знаний и практических умений обучающихся; углубление и расширение теоретических знаний; формирование умения использовать справочную литературу; развитие познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности и организованности; формирование самостоятельности мышления, способностей к саморазвитию; самосовершенствованию и самореализации; развитие исследовательских умений.

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.

Средство контроля, организованное как специальная беседа преподавателя обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное выяснение объема знаний обучающегося по определенному разделу, теме.
Темы вопросов по разделу 1:
1. Какие конкретные признаки аномальной активности обнаруживаются при анализе сетевого трафика?
2. Какие методы используются для классификации обнаруженных аномалий как потенциальных угроз безопасности?
3. Чем система IDS отличается от системы IPS в контексте обнаружения и блокирования атак?
Темы вопросов по разделу 2:
1. Мониторинг каких журналов осуществляется для выявления аномальной активности?
2. Как определить, что определенная запись в журнале может указывать на потенциальную угрозу безопасности?
3. Как часто проводится анализ журналов для обнаружения аномалий и угроз?
Темы вопросов по разделу 3:
1. Какие типы атак систем IDS и IPS способны обнаруживать и блокировать, и как они работают в синергии для защиты сети?
2. Какие преимущества и недостатки имеет использование систем IDS и IPS для обнаружения и предотвращения атак?
3. Какие дополнительные меры безопасности необходимо принять после обнаружения и блокирования атак с помощью IDS и IPS?
Темы вопросов по разделу 4:
1. Какие инструменты сканирования приложений необходимо использовать для выявления уязвимостей, и как часто проводить сканирование?
2. Как определяется приоритет устранения уязвимостей после их обнаружения?
3. Какие шаги необходимо предпринять после обнаружения критических уязвимостей в приложениях?
Темы вопросов по разделу 5:
1. Какие параметры безопасности операционных систем необходимо проанализировать, чтобы гарантировать их безопасность?
2. Как необходимо отреагировать на обнаружение потенциальных угроз безопасности операционных систем?
3. Какие инструменты необходимо использовать для сбора данных о безопасности операционных систем?
Темы вопросов по разделу 6:
1. Какие методы анализа угроз на уровне приложений применяются для обнаружения возможных атак?
2. Как оценивается степень угрозы на уровне приложений и принимаются меры по ее снижению?
3. Как часто необходимо проводите анализ угроз на уровне приложений?
Темы вопросов по разделу 7:
1. Какие инструменты для анализа угроз на основе поведения необходимо использовать, и какие типы поведения считаются наиболее подозрительными?
2. Как можно определить, что конкретное поведение может указывать на потенциальную угрозу безопасности?
3. Какие шаги необходимо предпринять после обнаружения подозрительного поведения с помощью инструментов для анализа угроз на основе поведения?
Темы вопросов по разделу 8:
1. В каких случаях применение машинного обучения оправдано в области анализа угроз?

2. Какие типы алгоритмов машинного обучения необходимо использовать для обнаружения и классификации угроз?
3. Какие преимущества и недостатки имеет использование машинного обучения для анализа угроз?

Критерии оценивания.

В ходе устного опроса студент способен давать обоснованные ответы на вопросы и демонстрирует владение информацией по соответствующему тематическому разделу.

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
ПКС-3.2	Обоснованно выбирает технологии сбора и анализа сведений для обнаружения возможных атак и уязвимостей информационных систем и способен их применять.	Устное собеседование по теоретическим вопросам и выполнение практического задания

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 7, Типовые оценочные средства для проведения дифференцированного зачета по дисциплине

6.2.2.1.1 Описание процедуры

В ходе проведения зачета студенту предлагается выбрать билет содержащий два вопроса, после чего ему предоставляется 10 минут для подготовки ответов.
Список вопросов к экзамену:
1. Методы анализа сетевого трафика для обнаружения аномалий?
2. Типы угроз, которые выявляются при анализе сетевого трафика
3. Нормальное поведение сети для выявления аномалий
4. Инструменты и технологии анализа сетевого трафика
5. Наиболее важные журналы и логи для мониторинга безопасности
6. Инструменты мониторинга и анализа журналов
7. Определение аномальной активности на основе данных из журналов
8. Какая разница между системами IDS и IPS? Как они взаимодействуют друг другом?
9. Какие типы атак могут быть обнаружены и заблокированы системами IDS и IPS?
10. Критерии реагирования на обнаруженные угрозы с помощью IDS и IPS
11. Эффективность систем IDS и IPS в предотвращении атак.
12. Инструменты сканирования приложений на уязвимости.
13. Какие типы уязвимостей чаще всего обнаруживаются при сканировании приложений?
14. Оценка критичности уязвимостей и план их устранения

15. Как происходит защита приложений от уязвимостей?
16. Какие данные о безопасности операционных систем необходимо собирать и анализировать?
17. Какие метрики безопасности операционных систем считаются наиболее важными для мониторинга?
18. Как определяются уязвимости и потенциальные угрозы на основе данных безопасности операционных систем?
19. Какие шаги необходимо предпринять для улучшения безопасности операционных систем на основе анализа данных?
20. Методы анализа угроз на уровне приложений
21. Наиболее опасные типы угроз на прикладном уровне
22. Оценка рисков и уязвимостей приложений при анализе угроз на этом уровне
23. Меры безопасности для защиты приложений от известных и новых угроз
24. Инструменты анализа угроз на основе поведения
25. Нормальное поведение системы/пользователя для выявления аномалий.
26. Реагирование на обнаруженные аномалии, выявленные с помощью инструментов анализа поведения.
27. Преимущества в использовании инструментов анализа угроз на основе поведения по сравнению с другими методами.
28. Решение задач в области анализа угроз с использованием методов машинного обучения?
29. Какие типы алгоритмов машинного обучения применяются для обнаружения и классификации угроз?
30. Как происходит обучение моделей машинного обучения на данных об информационной безопасности?
31. Какие вызовы и проблемы возникают при применении машинного обучения в области анализа угроз и как они решаются?

Пример задания:

Вопрос 1. Наиболее опасные типы угроз на прикладном уровне
Вопрос 2. Какие типы атак могут быть обнаружены и заблокированы системами IDS и IPS?

6.2.2.1.2 Критерии оценивания

Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
На оба вопроса из билета даны правильные ответы, логически выстроены, использована профессиональная терминология. Обучающийся правильно интерпретирует полученный результат.	На один из вопросов билета студент дает неполный или неверный ответ, но с помощью наводящих вопросов исправляет и дает правильный, логически выстроенный ответ, используя профессиональну	Ответы на вопросы билета неполные, неуверенные, студент путается в терминах профессиональной терминологии, демонстрирует понимание задаваемых вопросов.	Студент дает неверные ответы на вопросы или демонстрирует непонимание сущности задаваемых вопросов.

	ю терминологию. Обучающийся в целом правильно интерпретирует полученные результаты.		

7 **Основная учебная литература**

1. 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.

2. Прохорова О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова, 2022. - 124.

8 Дополнительная учебная литература и справочная

1. Нагаев И. В. Информационная безопасность и защита информации [Электронный ресурс] : учебно-методическое пособие для бакалавров технических вузов / И. В. Нагаев, 2012. - 213.

2. Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин, 2017. - 701.

3. Попова Е. С. Информационная безопасность и защита информации [Электронный ресурс] : курс лекций / Е. С. Попова, 2009. - 68.

4. 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.

5. Ерохин В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко, 2015. - 182.

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. MS Office Professional Plus Education ALNG

2. Microsoft Windows Seven Professional (Microsoft Windows Seven Starter) - Seven, Vista, XP_prof_64, XP_prof_32 - поставка 2010

12 Материально-техническое обеспечение дисциплины

1. Рабочая станция: ASUS PSQ-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. Оверхед-проектор GEHA OHP Top vision 800