Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Технология сбора и анализа информации

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2023 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	8			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	44	44	44	44
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): к.э.н., доцент, Бондаренко Г. А.

Зав. кафедрой: к.э.н., доцент Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	ознакомление навыкам и методам эффективного сбора, обработки и анализа информации, необходимой для выявления угроз и уязвимостей в информационных системах

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-5: способен организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять защитой объектов информатизации

В результате освоения дисциплины обучающийся должен:

Знать:

- принципы и стандарты, регулирующих информационную безопасность.
- разнообразные подходы к сбору, хранению и обработке данных, в том числе открытых источников (OSINT).
- методы и инструменты выявления уязвимостей в программных и аппаратных системах.
- норм и правил, регулирующих деятельность в сфере обработки и защиты информации.

(соотнесено с индикатором ПК-5.1)

Уметь:

- интерпретировать и визуализировать результаты анализа для принятия решений.
- проводить оценку текущего состояния систем безопасности и их уязвимостей.
- разрабатывать стратегии и тактики защиты информации в зависимости от выявленных рисков.
- оперативно реагировать на инциденты безопасности и минимизировать их последствия.

(соотнесено с индикатором ПК-5.2)

Владеть:

- работы со специализированным ПО и инструментами для сбора и анализа данных
- оценки информации и выявления ложных или недостоверных данных
- подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности

(соотнесено с индикатором ПК-5.2)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Теоретические и методические аспекты осуществления сбора и анализа данных в рамках информационной безопасности

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Введение в технологии сбора данных в рамках осуществления информационной безопасности объекта. Понятие информационной безопасности, её значение в современном мире. Значение процесса сбора данных для выявления уязвимостей и угроз информационной безопасности. Обзор текущих вызовов и тенденций в информационной безопасности. / Лек /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.2	Введение в технологии сбора данных в рамках осуществления информационной безопасности объекта. Проведение исследования о значении информационной безопасности в современном мире. Выбор объекта исследования и анализ его подходов к обеспечению информационной безопасности. / Пр /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.3	Введение в технологии сбора данных в рамках осуществления информационной безопасности объекта. Виды кибератак: фишинг, DDoS-атаки, зловредное ПО, insider threats и др. Реальные примеры инцидентов безопасности. Влияние информационной безопасности на репутацию компании. Финансовые последствия утечки данных. / Ср /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.4	Открытые источники информации (OSINT) Определение открытых источников информации, их виды и значение в кибербезопасности. Примеры использования OSINT для расследования инцидентов (сайты, социальные сети, базы данных). Обзор популярных инструментов для сбора OSINT. / Лек /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.5	Открытые источники информации (OSINT)	8	4	ПК-5	Л1.1, Л1.2, Л1.3,

	Разработка плана OSINT-исследования по заданной теме (например, анализ публичных профилей в социальных сетях). Сбор информации и представление результатов в виде презентации (5-10 слайдов), включая используемые источники и методы. / Пр /				Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.6	Открытые источники информации (OSINT). Преимущества и недостатки OSINT по сравнению с другими методами Текущие тренды и технологии, оказывающие влияние на развитие OSINT. Тренды в развитии социальных сетей и влияние данных тенденций на сбор информации. / Ср /	8	6	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.7	Методология сбора информации для обеспечения информационной безопасности Этапы сбора данных: планирование, реализация, анализ и отчетность. Различные методологии (качественные/количественные подходы) к сбору данных и направления их применения. / Лек /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.8	Методология сбора информации для обеспечения информационной безопасности Разработка методики сбора данных для конкретной ситуации (например, для оценки уязвимостей в системе). Подготовка плана действий, описание и обоснование применения выбранных методов и описание ожидаемых результатов / Пр /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.9	Примеры применения различных методик сбора информации в реальных ситуациях. Рассмотрение случаев неправильного применения методик сбора данных. Обеспечение качества данных Подходы к обеспечению точности и достоверности собранной информации. Методы обеспечения контроля за качеством данных на всех этапах. Этика и конфиденциальность Тренды в методологиях сбора информации / Ср /	8	6	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.10	Этические и правовые аспекты сбора данных Рассмотрение законодательства в области сбора данных. Этические нормы и дилеммы в работе с данными. Рассмотрение реальных примеров нарушения этики. / Лек /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.11	Этические и правовые аспекты сбора данных Анализ этического аспекта текущего случая в СМИ, связанного с нарушением прав при сборе данных. Рассмотрение и анализ последствий и предложений по улучшению практик сбора данных / Пр /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.12	Этические и правовые аспекты сбора данных Рассмотрение вопросов влияния различий в законодательстве о защите данных на международные компании. Исследование вопроса, в каких странах действуют наиболее строгие нормы в сфере сбора данных и почему. Перспективы развития правовых и этических норм в области защиты данных в будущем. Рассмотрение потенциальных изменений, которые могут произойти в законодательстве из-за технологических изменений и общественного мнения. / Ср /	8	6	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 2. Практические аспекты осуществления сбора и анализа данных в рамках информационной безопасности

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Основы мониторинга систем информационной безопасности и сбора логов Введение в логирование: что такое логи и зачем они нужны. Разновидности логов: системные, сетевые, приложения. Принципы сбора и хранения логов, включая стандарты. Значение анализа логов в информационной безопасности: Роль анализа логов в выявлении инцидентов и угроз.	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

	Основные техники анализа: корреляция, паттерны, аномалии. Примеры использования логов для расследования инцидентов. / Лек /				
2.2	Основы мониторинга систем информационной безопасности и сбора логов Ознакомление с принципами работы с логами, анализа и выявления возможных инцидентов и угроз на основе логов. / Пр /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.3	Основы мониторинга систем информационной безопасности и сбора логов. Изучение конкретных случаев и примеров из реальной жизни, где анализ логов привел к успешному выявлению инцидентов. Исследование будущих трендов в логировании и мониторинге, такие как машинное обучение и автоматизация. / Ср /	8	6	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.4	Применение методов и технологий для анализа сетевого трафика и выявления аномалий. Определение и цель осуществления мониторинга сети. Методы мониторинга. Инструменты для мониторинга и анализа информационной безопасности. Анализ аномалий. Направления и практика применения мониторинга сети. / Лек /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.5	Применение методов и технологий для анализа сетевого трафика и выявления аномалий. Применение инструментов мониторинга сети для анализа трафика, выявления аномалий и формирования отчетов по безопасности. / Пр /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.6	Применение методов и технологий для анализа сетевого трафика и выявления аномалий. Рассмотрение направлений применения организациями разных секторов (финансовый, медицинский, промышленный) мониторинга сети для достижения своих целей безопасности. Какие известные инциденты безопасности были предотвращены или выявлены с помощью мониторинга сети? / Ср /	8	6	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.7	Алгоритм сбора данных по информационной безопасности на основе опросов. Определение цели опроса. Разработка опросника. Выбор целевой аудитории. Выбор метода сбора данных. Проведение опроса. Сбор и хранение данных. Анализ данных. Подготовка отчета. Обратная связь и корректировка / Лек /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.8	Алгоритм сбора данных по информационной безопасности на основе опросов. Разработка и проведение опрос для сбора данных о состоянии информационной безопасности в организации, анализ полученных результатов / Пр /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.9	Алгоритм сбора данных по информационной безопасности на основе опросов. Организация эффективного процесса сбора данных по информационной безопасности на основе опросов, разработка надежных мер по защите информации на основе результатов проведенных опросов / Ср /	8	6	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.10	Технология сбора информации при осуществлении документооборота в компании в рамках обеспечения информационной безопасности. Определение типов документов. Классификация документов по уровню чувствительности (например, конфиденциальные, ограниченного доступа, открытые). Правила хранения и передачи для каждого типа документа. Автоматизация документооборота. Использование электронной подписи для повышения безопасности и упрощения процесса согласования документов. Безопасные каналы передачи данных. Контроль доступа. Мониторинг и аудит документооборота. Разработка инструкции по безопасной работе с конфиденциальными документами. Хранение и резервное копирование. Разработка и внедрение внутренней политики по документообороту, касающиеся обработки и хранения документов. / Лек /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.11	Технология сбора информации при осуществлении	8	4	ПК-5	Л1.1, Л1.2, Л1.3,

	документооборота в компании в рамках обеспечения информационной безопасности. Анализ и повышение эффективности документооборота в компании. Изучение технологий и подходов к обеспечению информационной безопасности в документообороте. Оценка существующих процессов документооборота в компании. Разработка рекомендаций по повышению эффективности процесса документооборота / Пр /				Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.12	Технология сбора информации при осуществлении документооборота в компании в рамках обеспечения информационной безопасности. Рассмотрение лучших практик управления доступом к документам в организации. Риски, связанные с электронным документооборотом и минимизация их последствий. Влияние технологии облачного хранения и передачи данных на безопасность документооборота. / Ср /	8	4	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 3. Промежуточная аттестация

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
3.1	Зачет / Зачёт /	8	0	ПК-5	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Аверченков В. И.	Аудит информационной безопасности: учебное пособие	Москва: ФЛИНТА, 2021	https://biblioclub.ru/index.php?page=book&id=93245 неограниченный доступ для зарегистрированных пользователей
Л1.2	Тищенко П. А., Казаков Ю. М., Филиппов Р. А., Филиппова Л. Б., Кузьменко А. А., Тищенко А. А.	Безопасность электронного документооборота: учебное пособие	Москва, Берлин: Директ-Медиа, 2021	https://biblioclub.ru/index.php?page=book&id=602225 неограниченный доступ для зарегистрированных пользователей
Л1.3	Мирошников, А. И., Сысоев, А. С.	Основы информационной безопасности и защита информации: учебное пособие	Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2022	https://www.iprbookshop.ru/128718.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Киренберг, А. Г.	Информационная безопасность современных операционных систем: учебное пособие	Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022	https://www.iprbookshop.ru/128393.html неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.5	Ванина, А. Г., Минкина, Т. В.	Гуманитарные проблемы обеспечения информационной безопасности: учебное пособие (курс лекций)	Ставрополь: Северо-Кавказский федеральный университет, 2021	https://www.iprbookshop.ru/135681.html неограниченный доступ для зарегистрированных пользователей
Л1.6	Бондарчук Н. В.	Бизнес-разведка: практикум: учебное пособие	Москва: Дашков и К°, 2022	https://biblioclub.ru/index.php?page=book&id=696968 неограниченный доступ для зарегистрированных пользователей
Л1.7	Трайнев В. А.	Системный подход к обеспечению информационной безопасности предприятия (фирмы): монография	Москва: Дашков и К°, 2022	https://biblioclub.ru/index.php?page=book&id=698555 неограниченный доступ для зарегистрированных пользователей
Л1.8	Трайнев В. А.	Совершенствование информационной системы организации управления предприятием, объединением: отечественная практика: монография	Москва: Дашков и К°, 2023	https://biblioclub.ru/index.php?page=book&id=698559 неограниченный доступ для зарегистрированных пользователей
Л1.9	Щерба Е. В., Щерба М. В., Магазев А. А., Маер О. В.	Противодействие сетевым атакам в локальных сетях: учебное пособие	Омск: Омский государственный технический университет (ОмГТУ), 2021	https://biblioclub.ru/index.php?page=book&id=700833 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2014	https://biblioclub.ru/index.php?page=book&id=238446 неограниченный доступ для зарегистрированных пользователей
Л2.2	Аверченков В. И., Рытов М. Ю., Кондрашин Г. В., Рудановский М. В.	Системы защиты информации в ведущих зарубежных странах: учебное пособие	Москва: ФЛИНТА, 2021	https://biblioclub.ru/index.php?page=book&id=93351 неограниченный доступ для зарегистрированных пользователей
Л2.3	Аверченков В. И., Рытов М. Ю.	Служба защиты информации: организация и управление: учебное пособие	Москва: ФЛИНТА, 2021	https://biblioclub.ru/index.php?page=book&id=93356 неограниченный доступ для зарегистрированных пользователей
Л2.4	Лукаш Ю. А.	Бизнес-разведка как составляющая обеспечения безопасности и развития бизнеса: учебное пособие	Москва: ФЛИНТА, 2017	https://biblioclub.ru/index.php?page=book&id=114954 неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.5	Беловицкий, К. Б.	Коммерческий шпионаж (противодействие): учебное пособие	Москва: Научный консультант, 2020	https://www.iprbookshop.ru/110596.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

ИСС "КонсультантПлюс"
База данных действующих стандартов по направлению "Информационная Безопасность" https://www.gost.ru/portal/gost/home/standarts/InformationSecurity
Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)//fstec.ru

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
LibreOffice

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-5: способен организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять защитой объектов информатизации			
З - принципы и стандарты, регулирующих информационную безопасность. - разнообразные подходы к сбору, хранению и обработке данных, в том числе открытых источников (OSINT). - методы и инструменты выявления уязвимостей в программных и аппаратных системах. - норм и правил, регулирующих деятельность в сфере обработки и защиты информации.	Демонстрирует понимание особенностей применения стандартов информационной безопасности в рамках сбора данных, описывает основные подходы к сбору, хранению и обработке данных, методы и инструменты выявления уязвимостей, нормы и правила обработки информации для подготовки к зачету, опросу	Полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие ответов материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет	О – (1-65) ВЗ– (1-32)
У - интерпретировать и визуализировать результаты анализа для принятия решений. - проводить оценку текущего состояния систем безопасности и их уязвимостей. - разрабатывать стратегии и тактики защиты информации в зависимости от выявленных рисков. - оперативно реагировать на инциденты безопасности и минимизировать их последствия.	Осуществляет оценку состояния систем безопасности, анализ угроз и уязвимостей, оперативное реагирование на инциденты безопасности, разработку стратегии и тактики защиты информации на основе собранных данных в процессе выполнения практико-ориентированного и задания к зачету	Полнота и содержательность выполненного практико-ориентированного задания; обоснованность обращения к профессиональным базам;	ПОЗ – (1-8) ЗЗ – (1-10)
В – навыками - работы со специализированным ПО и инструментами для сбора и анализа данных	Использует инструменты для сбора и анализа данных, производит оценку информации и выявляет ложные и недостоверные данные, осуществляет поиск и подбор	Полнота и содержательность выполненного практико-ориентированного задания, глубина анализа; использование различных	ПОЗ – (1-8) ЗЗ – (1-10)

- оценки информации и выявления ложных или недостоверных данных - подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности	нормативных и методических материалов по вопросам обеспечения информационной безопасности в процессе выполнения практико-ориентированного и задания к зачету	источников информации Интернет ресурсов, в целях осуществления определенных этапов информационно-аналитической деятельности;	

О – опрос, ВЗ – вопросы к зачету, ПОЗ - практико-ориентированные задания, ЗЗ – задания к зачету

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

50-100 баллов – «зачтено»
0-49 баллов – «не зачтено»

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету

1. Что такое информационная безопасность и почему она важна в современном мире?
2. Опишите основные компоненты информационной безопасности.
3. Как сбор данных способствует выявлению уязвимостей и угроз информационной безопасности?
4. Какие текущие вызовы стоят перед информационной безопасностью?
5. Что такое открытые источники информации (OSINT)? Приведите примеры.
6. В каких сферах кибербезопасности применяется OSINT?
7. Какие типы открытых источников информации можно использовать для расследования инцидентов?
8. Назовите популярные инструменты для сбора OSINT и кратко опишите их функционал.
9. Каковы основные этапы сбора данных для обеспечения информационной безопасности?
10. В чем разница между качественными и количественными методами сбора данных?
11. Каковы ключевые моменты в процессе анализа и отчетности по собранным данным?
12. Какое законодательство регулирует сбор данных в области информационной безопасности?
13. Какие этические нормы должны соблюдать специалисты по информационной безопасности при работе с данными?
14. Приведите примеры нарушения этики в процессе сбора данных.
15. Что такое логи и зачем они нужны в информационной безопасности?
16. Какие существуют виды логов? Приведите примеры для каждого типа.
17. Каковы основные принципы сбора и хранения логов?
18. Объясните, как анализ логов помогает в выявлении инцидентов и угроз.
19. Каковы цели осуществления мониторинга сети?
20. Какие методы используются для мониторинга сетевого трафика?
21. Назовите инструменты для анализа и мониторинга информационной безопасности.
22. Какие техники используются для анализа аномалий в сетевом трафике?
23. Как определить цель опроса в области информационной безопасности?
24. Каковы основные этапы разработки и проведения опроса?
25. Как происходит анализ данных, собранных в результате опроса?
26. Каковы основные типы документов, используемых в документообороте?
27. Как классифицировать документы по уровню чувствительности? Приведите примеры.
28. Как автоматизация документооборота может повысить безопасность обработки документов?
29. Какая роль электронной подписи в обеспечении безопасности документооборота?

30. Какие ключевые аспекты следует учитывать при разработке внутренней политики по документообороту?
31. Как обеспечить контроль доступа и мониторинг документооборота в организации?
32. Объясните важность резервного копирования для безопасного хранения документов.

***Критерии оценивания*:**
Каждый вопрос оценивается отдельно, максимально в 30 баллов.
Критерии оценивания ответа на отдельный вопрос:

- 25 – 30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;
- 20 – 24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;
- 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
- 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Задания к зачету

Задание 1. Исследование угроз
Выберите известный случай утечек данных (например, утечка компании Target или Equifax). Напишите краткий анализ инцидента, указав основные уязвимости, использованные хакерами, и меры, которые могли бы предотвратить инцидент.

Задание 2. Использование OSINT
Проведите исследование с использованием открытых источников информации (OSINT) для выявления потенциально уязвимой организации. Используйте инструменты, такие как Maltego или Shodan, и представьте свой отчет, включая список обнаруженных уязвимостей и источников информации.

Задание 3. Методология сбора данных
Разработайте план сбора данных для оценки уровня информационной безопасности в выбранной организации. Укажите этапы сбора данных, методы, которые вы будете использовать, и возможные источники информации.

Задание 4. Этическое расследование
Опишите сценарий, в котором учет этических норм при сборе данных мог бы быть нарушен. Обсудите последствия такого нарушения и возможные меры по предотвращению подобных ситуаций в будущем.

Задание 5. Логирование и анализ
Создайте сценарий, в котором вам требуется анализ логов для выявления инцидента безопасности. Предоставьте пример логов и укажите, как вы будете выявлять аномалии или подозрительную активность. Опишите свои выводы.

Задание 6. Мониторинг сети
Разработайте проект мониторинга сети для гипотетической компании. Укажите методы мониторинга, инструменты, которые будете использовать, и опишите, как будете реагировать на выявленные аномалии.

Задание 7. Проведение опроса

Составьте анкету для проведения опроса среди сотрудников компании о восприятии информационной безопасности. Определите цели опроса, целевую аудиторию и методы анализа данных после его завершения.

Задание 8. Документооборот и безопасность
Разработайте внутреннюю политику по безопасному документообороту для гипотетической компании. Укажите классификацию документов, правила хранения и передачи, а также меры по обеспечению безопасности.

Задание 9. Практика использования электронной подписи
Создайте шаг за шагом инструкцию по внедрению электронной подписи для повышения безопасности документооборота в организации. Опишите, как это повлияет на процесс согласования документов и что необходимо для реализации этого решения.

Задание 10. Резервное копирование и защита данных
Предложите стратегию резервного копирования для компании, учитывая разные уровни чувствительности данных. Укажите частоту резервного копирования, способы хранения и меры по защите резервных копий.

Критерии оценивания задания:
- 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы, проведен анализ, дана грамотная интерпретация полученных результатов, сделаны выводы.
- 25-34 балла выставляется, если задание решено полностью, но при анализе и интерпретации полученных результатов допущены незначительные ошибки, выводы – достаточно обоснованы, но неполны.
- 11-24 балла выставляется, если задание решено частично, анализ и интерпретация полученных результатов не вполне верны, выводы верны частично.
- 0-10 баллов выставляется, если решение неверно или отсутствует.

Критерии оценивания:
Максимальное количество баллов 100. Каждое зачетное задание содержит 2 вопроса из перечня вопросов к зачету и 1 задание из перечня заданий к зачету. Ответ на каждый теоретический вопрос оценивается отдельно, максимально 30 баллов каждый. Задание оценивается максимально 40 баллов.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:
– 50-100 баллов (зачтено);
– 0-49 баллов (не зачтено).

Опрос

Вопросы для проведения опроса
1. Как вы определяете информационную безопасность в контексте современной организации?
2. Почему информационная безопасность является критически важной в цифровом мире?
3. Какие основные компоненты информационной безопасности вы можете выделить?
4. Каковы последствия нарушения информационной безопасности для компании?
5. Какие аспекты человеческого фактора влияют на информационную безопасность?
6. Как сбор данных может улучшить защиту информации в организации?
7. Какие типы данных наиболее важны для анализа уязвимостей?
8. Как часто необходимо проводить сбор данных для оценки информационной безопасности?
9. Какие методы сбора данных вы считаете наиболее эффективными?
10. Как можно использовать собранные данные для предсказания угроз?
11. Какие новые технологии создают угрозы для информационной безопасности?

12. Как изменение методов работы (например, работа на удалёнке) влияет на безопасность данных?
13. Какие киберугрозы, по вашему мнению, будут наиболее распространены в следующем году?
14. Как состояния мировых конфликтов могут влиять на информационную безопасность?
15. В какой мере законы и regulation-и влияют на подходы к кибербезопасности?
16. Какие виды открытых источников информации вы знаете?
17. Как вы определяете, какие источники являются надежными при проведении OSINT?
18. Приведите пример успешного применения OSINT в расследовании киберинцидента.
19. Какие инструменты для сбора OSINT вы считаете наиболее полезными и почему?
20. Как OSINT может быть использован для предупреждения угроз?
21. Как вы выбираете инструменты для сбора OSINT?
22. Какие функции должны быть у эффективного инструмента OSINT?
23. Каковы основные возможности и ограничения популярных инструментов OSINT?
24. Как инструменты OSINT могут помочь в анализе социальных сетей?
25. Как вы оцениваете актуальные тренды в разработке OSINT-инструментов?
26. Какие этапы включает в себя процесс сбора данных?
27. Как вы определяете, какие методологии (качественные или количественные) использовать?
28. Какие инструменты помогают в планировании процесса сбора данных?
29. Как провести анализ собранных данных и что вы можете извлечь из него?
30. Какова роль отчетности в процессе сбора данных?
31. Какие основные законы регулируют сбор данных в вашей стране?
32. Как вы считаете, должны ли организации соблюдать дополнительные этические стандарты?
33. Каковы примеры этических дилемм, с которыми могут столкнуться специалисты по информационной безопасности?
34. Как важно иметь внутренние политики для обеспечения этики в работе с данными?
35. Как закон о защите данных (например, GDPR) влияет на процесс сбора информации?
36. Почему логирование является важной частью управления информационной безопасностью?
37. Какие виды логов вы можете перечислить и какие их особенности?
38. Как часто следует проверять логи для выявления инцидентов?
39. Как можно улучшить процессы сбора и хранения логов?
40. Какие технические средства вы используете для анализа логов?
41. Каковы основные цели анализа логов в контексте информационной безопасности?
42. Какие техники анализа логов вы считаете наиболее эффективными?
43. Каков процесс корреляции событий из логов?
44. Как вы определяете аномалии в логах и что с ними делать?
45. Приведите пример того, как анализ логов помог обнаружить инцидент.
46. Какие основные методы мониторинга сети вы знаете?
47. Каковы преимущества проактивного мониторинга по сравнению с реактивным?
48. Какие инструменты вы считаете наиболее эффективными для мониторинга сетевой активности?
49. Какова роль мониторинга в предотвращении угроз?
50. Как вы измеряете эффективность мониторинга сети?

51. Как вы определяете цель проведения опроса в области информационной безопасности?
52. Какие ключевые вопросы вы бы включили в опрос для оценки уровня безопасности в компании?
53. Как выбрать целевую аудиторию для опроса?
54. Как вы обрабатываете и храните данные, полученные в результате опроса?
55. Какова роль обратной связи в улучшении процедур сбора данных?
56. Какие типы документов существуют в системе документооборота?
57. Как вы классифицируете документы по уровню чувствительности?
58. Каковы лучшие практики хранения и передачи различных типов документов?
59. Какие меры вы принимаете для автоматизации документооборота?
60. Как контролировать доступ к конфиденциальным документам?
61. Как использование электронной подписи повышает безопасность документооборота?
62. Какие риски связаны с неправомерным использованием электронной подписи?

63. Каковы преимущества и недостатки различных систем электронной подписи?
64. Какое законодательство регулирует использование электронной подписи в вашей стране?
65. Какой порядок внедрения электронной подписи в организацию вы бы предложили?

Критерии оценивания
Максимальное количество баллов – 20.
Студент может ответить на 20 вопросов. Ответ на каждый вопрос оценивается максимум в 1 балл.
Критерии оценивания одного вопроса:
правильный и полный ответ на 1 вопрос – 1 балл;
неправильный ответ на 1 вопрос – 0 баллов.

Практико-ориентированные задания

Задание 1.
Проведение исследования о значении информационной безопасности в современном мире. Выбор объекта исследования и анализ его подходов к обеспечению информационной безопасности.
1. Определение темы и целей исследования
   - Сформулировать тему работы.
   - Установить цели и задачи исследования.
2. Изучение литературы
   - Собрать материалы по информационной безопасности, современным угрозам и технологиям сбора данных.
   - Ознакомиться с существующими исследованиями и подходами.
3. Выбор объекта исследования
   - Определить организацию или систему для анализа.
   - Подготовить обоснование выбора.
4. Сбор и анализ данных
   - Исследовать подходы объекта к информационной безопасности.
   - Определить используемые технологии и методы сбора данных.
5. Оценка эффективности мер безопасности
   - Проанализировать, как объект оценивает свою безопасность.
   - Исследовать применяемые метрики и методы анализа.
6. Формулирование выводов и рекомендаций

Задание 2.
Разработка плана OSINT-исследования по заданной теме (например, анализ публичных профилей в социальных сетях). Сбор информации и представление результатов в виде презентации (5-10 слайдов), включая используемые источники и методы.
1. Определение цели и задач исследования
   - Сформулировать, что именно нужно выяснить (например, анализ сетевого поведения, выявление связей и интересов и т.д.).

2. Выбор объектов исследования
   - Определить, какие публичные профили или группы в социальных сетях будут анализироваться.
3. Методы сбора информации
   - Определить методы и инструменты для сбора данных:
     - Использование специализированных OSINT-инструментов.
     - Сбор данных вручную (скриншоты, заметки).
     - Анализ публикаций, комментариев и активностей пользователей.
4. Анализ данных
   - Систематизировать собранные данные.
   - Выявить закономерности, тренды и важные факты.
   - Оценить достоверность информации.
5. Подготовка результатов
   - Сформировать выводы на основе проведенного анализа.

- Подготовить рекомендации (например, как улучшить безопасность профиля).

6. Создание презентации
   - Оформить 5-10 слайдов:
     - Введение (цели и задачи).
     - Описание методов исследования.
     - Основные результаты и выводы.
     - Использованные источники и инструменты.
     - Заключение и рекомендации.

Задание 3.

Разработка методики сбора данных для конкретной ситуации (например, для оценки уязвимостей в системе). Подготовка плана действий, описание и обоснование применения выбранных методов и описание ожидаемых результатов.

1. Определение цели и задач
   - Выяснить, какие конкретные уязвимости необходимо оценить (например, уязвимости в веб-приложении, сетевой инфраструктуре и т.д.).
2. Анализ системы
   - Оценить структуру и архитектуру целевой системы для понимания её компонентов и взаимодействий.
   - Определить точки доступа и потенциальные векторы атаки.
3. Выбор методов сбора данных
   - Пасивный сбор данных:
     - Анализ открытых источников информации (OSINT).
     - Сканирование сетевых устройств и сервисов без воздействия на систему.
   - Активный сбор данных:
     - Пентестинг (тестирование на проникновение) для выявления уязвимостей.
     - Использование инструментов сканирования уязвимостей.
4. Разработка плана действий
   - Составить пошаговую инструкцию для выполнения сбора данных, включая:
     - Время проведения тестов.
     - Ответственные лица.
     - Условия тестирования (например, минимизация влияния на производительность).
5. Обоснование применения методов
   - Описать, почему выбранные методы наиболее подходящие для текущей ситуации (увязывание с целями исследования, специфичность уязвимостей).
6. Сбор и анализ данных
   - Провести сбор данных в соответствии с разработанным планом.
   - Систематизировать результаты, отфильтровать ложные срабатывания.
7. Ожидаемые результаты
   - Описание того, какие уязвимости могут быть выявлены.
   - Прогнозирование возможных рисков для системы.

8. Документация и отчет
   - Составить документ с описанием проведенных действий, выявленных уязвимостей и предложениями по их устранению.

Задание 4.

Анализ этического аспекта текущего случая в СМИ, связанного с нарушением прав при сборе данных. Рассмотрение и анализ последствий и предложений по улучшению практик сбора данных.

1. Выбор и описание случая
   - Определить конкретный случай из СМИ, связанный с нарушением прав при сборе данных (например, утечка личных данных, использование персональной информации без согласия).
2. Анализ этических принципов
   - Оценить, какие этические нормы и права были нарушены (например, право на конфиденциальность, право на информированное согласие).

- Рассмотреть влияние на индивидуумов и общество в целом.

3. Последствия нарушения прав
   - Проанализировать краткосрочные и долгосрочные последствия для пострадавших и организаций (например, потеря доверия, судебные иски, репутационные потери).
   - Обсудить влияние на общественное восприятие и законодательство в области защиты данных.
4. Сравнительный анализ
   - Изучить, как другие организации или страны решают подобные проблемы (успешные практики, случаи из истории).
5. Предложения по улучшению практик
   - Разработать рекомендации для организаций по улучшению практик сбора данных (например, внедрение прозрачных политик, регулярные тренинги для сотрудников).
   - Обсудить необходимость усиления законодательства и саморегулирования в сфере защиты данных.
6. Заключение
   - Подвести итоги анализа, подчеркнув важность соблюдения этических стандартов при сборе данных.
   - Отметить необходимость общественного контроля и социальной ответственности компаний.

Задание 5.

Ознакомление с принципами работы с логами, анализа и выявления возможных инцидентов и угроз на основе логов.

1. Сбор логов
   - Определить источники логирования (серверы, приложения, сетевые устройства).
   - Настроить центральный сбор логов для упрощенного анализа
2. Форматирование и нормализация данных
   - Ознакомиться с форматами логов (например, JSON, CSV, текстовые файлы).
   - Преобразовать данные в унифицированный формат для анализа.
3. Анализ логов
   - Использовать инструменты для анализа логов.
   - Осуществить фильтрацию и сортировку логов по временным меткам, уровню серьезности и источнику.
4. Выявление аномалий
   - Установить базовые параметры нормального поведения системы.
   - Идентифицировать отклонения от нормы (аномалии) путем анализа паттернов и исторических данных.
5. Определение инцидентов и угроз
   - Произвести количественный и качественный анализ событий для выявления потенциальных инцидентов.
   - Оценить серьезность угроз и их возможные последствия.
6. Документация и реагирование
   - Задокументировать все выявленные инциденты и предпринятые меры.
   - Разработать и внедрить план реагирования на инциденты (IRP).

7. Обратная связь и улучшение
   - Оценить эффективность процесса анализа и реагирования.
   - Внедрить изменения и улучшения в процессах логирования и мониторинга.

Задание 6.

Применение инструментов мониторинга сети для анализа трафика, выявления аномалий и формирования отчетов по безопасности.

1. Подготовка окружения
   - Установите виртуальную машину с операционной системой (рекомендуется Linux).
   - Обеспечьте доступ к сети для мониторинга.
2. Установка инструментов
   - Установите инструменты для мониторинга, такие как:
     - Wireshark для анализа сетевого трафика.

- Snort или Suricata для обнаружения и предотвращения вторжений.

3. Сбор сетевого трафика
   - Запустите Wireshark и начните захват трафика на выбранном сетевом интерфейсе.
   - Генерируйте различный сетевой трафик (например, веб-серфинг, передачи файлов) для анализа.
4. Анализ трафика
   - Используйте Wireshark для фильтрации и анализа захваченных данных.
   - Определите протоколы, источники и назначения трафика, а также объём передачи данных.
5. Выявление аномалий
   - Настройте Snort/Suricata для мониторинга трафика и обнаружения подозрительных активностей.
   - Проанализируйте сгенерированные отчеты о событиях для выявления аномалий (например, необычные IP-адреса, превышение норм нагрузки).
6. Формирование отчетов
   - Подготовьте отчет, включающий:
     - Описание проведенного анализа.
     - Выявленные аномалии и события безопасности.
     - Скриншоты и графики для визуализации данных.

Задание 7.

Разработка и проведение опрос для сбора данных о состоянии информационной безопасности в организации, анализ полученных результатов.

1. Определение целей опроса
   - Четко сформулируйте цели, которые необходимо достичь с помощью опроса. Например, оценка уровня осведомленности сотрудников о безопасности.
2. Разработка вопросов
   - Создайте вопросы, которые помогут получить нужную информацию. Вопросы могут быть разного типа:
     - Закрытые (с вариантами ответов).
     - Открытые (для свободного ответа).
   - Убедитесь, что вопросы понятны и логично связаны.
3. Выбор целевой аудитории
   - Определите, кто будет участвовать в опросе. Это могут быть разные группы сотрудников (ИТ, административный персонал и т.д.).
4. Проведение опроса
   - Выберите способ проведения (онлайн-анкеты, интервью) и распространите опросный лист среди участников.
   - Установите срок для заполнения анкеты, чтобы получить результаты в разумные сроки.
5. Сбор и обработка данных
   - Соберите все ответы и проведите их структурирование.
   - Используйте статистические методы или инструменты для анализа данных
6. Анализ результатов
   - Проанализируйте полученные данные, выделите ключевые моменты и тенденции.

Задание 8.

Анализ и повышение эффективности документооборота в компании. Изучение технологий и подходов к обеспечению информационной безопасности в документообороте. Оценка существующих процессов документооборота в компании. Разработка рекомендаций по повышению эффективности процесса документооборота.

1. Сбор информации о текущих процессах
   - Изучите существующие процессы документооборота в компании. Проведите интервью с ключевыми сотрудниками и соберите документацию.
2. Оценка технологий и инструментов
   - Исследуйте используемые в компании технологии и системы для документооборота, а также технологии обеспечения безопасности.
3. Анализ информационной безопасности
   - Оцените текущие меры по обеспечению информационной безопасности в документообороте: контроль доступа, шифрование, резервное копирование.

4. Выявление проблем и узких мест
- Определите недостатки и проблемы в процессах документооборота, такие как задержки, ошибки или недостаточная защита данных.
5. Сравнительный анализ
- Проведите сравнение с отраслевыми стандартами и лучшими практиками, чтобы определить любые пробелы в текущих процессах.
6. Разработка рекомендаций
- На основе проведенного анализа сформулируйте рекомендации по повышению эффективности, включая:
  - Автоматизацию процессов.
  - Обучение сотрудников.
  - Усовершенствование мер безопасности.
7. Подготовка отчета
- Создайте отчет, в котором будут изложены результаты анализа, выявленные проблемы и предложенные рекомендации.

Критерии оценивания отдельного практико-ориентированного задания:

Каждое практико-ориентированное задание оценивается максимально по 10 баллов каждое. Максимальное количество баллов за выполнение всех практико-ориентированных заданий – 80 баллов.

- 9-10 баллов выставляется, если обучающийся: выполнил задание в полном объеме, самостоятельно, с соблюдением необходимой последовательности; грамотно оформил представленный отчет;
- 6-8 баллов выставляется, если обучающийся: выполнил задание в полном объеме, самостоятельно, с соблюдением необходимой последовательности; грамотно оформил представленный отчет; дана содержательная интерпретация полученных при решении задач результатов; материал изложен четко; допускаются отдельные логические и стилистические погрешности, уверенно исправленные после дополнительных вопросов;
- 3-5 балла выставляется, если обучающийся: выполнил задание в полном объеме с соблюдением необходимой последовательности; грамотно оформил представленный отчет; дана содержательная интерпретация полученных результатов; допускаются отдельные логические и стилистические погрешности; обучающийся может испытывать некоторые затруднения в формулировке суждений;
- 0-2 балла выставляется, если задание не выполнено или выполнено не в полном объеме; обучающийся практически не владеет теоретическим материалом, допуская грубые ошибки, испытывает затруднения в формулировке собственных суждений, неспособен ответить на дополнительные вопросы.

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме - зачета.

Зачет проводится по расписанию промежуточной аттестации в устной форме. Количество вопросов в зачетном задании – 3 (2 теоретических вопроса и 1 задание). Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия.

В ходе лекционных занятий рассматриваются основные понятия в области информационно-аналитической работы в рамках информационной безопасности и защиты информации, методы обработки и анализа информации об инцидентах, возможных угрозах и рисках, даются рекомендации для самостоятельной работы и подготовки к практическим занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по информационно-аналитической работе в рамках информационной безопасности.

При подготовке к практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием практической работы;

В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных источников. Выделить непонятные термины и найти их значение в энциклопедических словарях.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.