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
Методология и организация информационно-аналитической деятельности

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 2022 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.к., доц. Радченко Ю.В.

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

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Целью дисциплины является освоение основных принципов организации, реализации и автоматизации информационно аналитической деятельности для решения профессиональных задач и принятия управленческих решений.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-3: способен проводить анализ информационной безопасности объектов и автоматизированных систем на соответствие требованиям стандартов в области информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

- стандарты информационной безопасности, методы оценки и аудита, основные угрозы и уязвимости, а также принципы интеграции методов защиты в бизнес-процессы и документирования политик безопасности (соотнесено с индикатором ПК -3.1)

Уметь:

- проводить анализ и аудит информационных систем, выявлять и оценивать риски информационной безопасности (соотнесено с индикатором ПК-3.2)

Владеть:

- подготовки аналитических отчетов и документации с рекомендациями по улучшению информационной безопасности (соотнесено с индикатором ПК-3.2)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Введение в информационно-аналитическую деятельность

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Введение в информационно-аналитическую деятельность. Этапы аналитического исследования. Задачи аналитиков информационной безопасности. Информационно-аналитические системы. Источники и типы данных, генерируемых в информационно-аналитических системах / Лек /	8	2	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.2	Введение в информационно-аналитическую деятельность. Этапы аналитического исследования. Задачи аналитиков информационной безопасности. Информационно-аналитические системы. Источники и типы данных, генерируемых в информационно-аналитических системах / Пр /	8	2	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.3	История и эволюция информационно-аналитической деятельности – ключевые этапы развития, роль технологий. Этика и правовые аспекты информационно-аналитической деятельности – защита данных, конфиденциальность и соблюдение законодательства. / Ср /	8	6	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.4	Алгоритм решения аналитических задач. Определение проблемы, постановка, цели, задач и гипотез исследования. Методы статистической обработки, анализа и прогнозирования: идентификация источников информации, сбор данных, предварительная обработка и анализ данных с помощью методов статистики; простейшие методы моделирования и прогнозирования. / Лек /	8	6	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.5	Алгоритм решения аналитических задач. Определение проблемы, постановка, цели, задач и гипотез исследования. Методы статистической обработки, анализа и прогнозирования: идентификация источников информации, сбор данных, предварительная обработка и анализ данных с помощью методов статистики; простейшие методы моделирования и прогнозирования с применением LibreOffice / Пр /	8	6	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.6	Технологии и инструменты анализа данных – программные решения для анализа и визуализации данных. Аналитика в	8	8	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6,

	разных областях – применение информационно-аналитической деятельности в бизнесе, государственном управлении, здравоохранении и других сферах. / Ср /				Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
Раздел 2. Мониторинг информационной безопасности					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
2.1	Мониторинг информационной безопасности: основные аспекты, этапы и направления. Управление рисками информационной безопасности: идентификация, оценка и управление. Экономическое обеспечение информационной безопасности: расчет и анализ финансовых показателей, связанных с защитой информации и активов организации, а также обоснование затрат на безопасность / Лек /	8	6	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.4, Л2.5
2.2	Мониторинг информационной безопасности: основные аспекты, этапы и направления. Управление рисками информационной безопасности: идентификация, оценка и управление. Экономическое обеспечение информационной безопасности: расчет и анализ финансовых показателей, связанных с защитой информации и активов организации, а также обоснование затрат на безопасность с применением LibreOffice / Пр /	8	6	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.3	Роль данных в принятии решений - влияние информации на стратегии и тактики оценки рисков и принятия управленческих решений. Ключевые показатели эффективности (KPI) и метрики для оценки работы системы безопасности и управления инцидентами. / Ср /	8	8	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.4	Подготовка аналитической и отчетной документации. Типы политики, процедур, инструкций, отчетов. Стандарты информационной безопасности. Аудит и оценка информационной безопасности. Формы и структура аналитических отчетов. Модель угроз. / Лек /	8	6	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.4, Л2.5
2.5	Подготовка аналитической и отчетной документации. Типы политики, процедур, инструкций, отчетов. Стандарты информационной безопасности. Аудит и оценка информационной безопасности. Формы и структура аналитических отчетов. Модель угроз. / Пр /	8	6	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.4, Л2.5
2.6	Циклы PDCA (Plan-Do-Check-Act). Создание и актуализация планов действий в случае инцидентов. Стратегии обеспечения непрерывности бизнес-процессов и восстановления после инцидентов / Ср /	8	8	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.4, Л2.5
Раздел 3. Методы машинного обучения в информационной безопасности					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
3.1	Методы машинного обучения в информационной безопасности. Типы машинного обучения (с учителем, без учителя, с подкреплением). Алгоритмы машинного обучения (линейная и логистическая регрессия, к-ближайших соседей, деревья решений, случайный лес, к-средних, метод главных компонент, факторный анализ). Метрики качества построенных моделей. Применение методов машинного обучения в информационной безопасности: обнаружение угроз, анализ поведения пользователей, защита от фишинга, обработка естественного языка. / Лек /	8	12	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.4, Л2.5
3.2	Методы машинного обучения в информационной безопасности. Типы машинного обучения (с учителем, без учителя, с подкреплением). Алгоритмы машинного обучения (линейная и логистическая регрессия, к-ближайших соседей, деревья решений, случайный лес, к-средних, метод главных компонент, факторный анализ). Метрики качества построенных моделей.	8	12	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.4, Л2.5

	Применение методов машинного обучения в информационной безопасности: обнаружение угроз, анализ поведения пользователей, защита от фишинга, обработка естественного языка на языке программирования Python с помощью Google Collab / Пр /				
3.3	Системы предотвращения и обнаружения вторжений (IPS/IDS). Анализ журналов событий. Идентификация инсайдерских угроз. Автоматизация реагирования на инциденты. Защита моделей машинного обучения. / Ср /	8	14	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, Л2.1, Л2.2, Л2.4, Л2.5

Раздел 4. Промежуточная аттестация

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
4.1	/ Зачёт /	8	0	ПК-3	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л1.6, Л1.7, Л1.8, Л1.9, Л1.10, Л1.11, Л1.12, Л1.13, 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	Сафонова, Л. А.	Экономические аспекты информационной безопасности: учебное пособие	Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2019	https://www.iprbookshop.ru/90606.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Голембиовская, О. М., Рытов, М. Ю., Шинаков, К. Е.	Формализация подходов к обеспечению защиты персональных данных: монография	Саратов: Ай Пи Эр Медиа, 2019	https://www.iprbookshop.ru/81851.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Шинаков, К. Е., Рытов, М. Ю., Голембиовская, О. М.	Анализ рисков безопасности информационных систем персональных данных: монография	Москва: Ай Пи Ар Медиа, 2020	https://www.iprbookshop.ru/95150.html неограниченный доступ для зарегистрированных пользователей
Л1.5	Галатенко, В. А.	Основы информационной безопасности: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	https://www.iprbookshop.ru/97562.html неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.6	Голембиовская, О. М., Рытов, М. Ю., Голембиовский, М. М., Шинаков, К. Е., Банников, А. И., Кондрашова, Е. В., Дорошенко, В. Ю.	Формализация подхода к определению актуальности угроз информационной безопасности: монография	Саратов: Вузовское образование, 2022	https://www.iprbookshop.ru/121143.html неограниченный доступ для зарегистрированных пользователей
Л1.7	Целых, А. Н., Целых, Л. А.	Современные программные сервисы информационно-аналитической деятельности: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2023	https://www.iprbookshop.ru/133478.html неограниченный доступ для зарегистрированных пользователей
Л1.8	Голембиовская, О. М., Рытов, М. Ю., Шинаков, К. Е., Горлов, А. П., Губсков, Ю. А., Голембиовский, М. М., Кондрашова, Е. В.	Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации: учебное пособие	Саратов: Вузовское образование, 2024	https://www.iprbookshop.ru/134999.html неограниченный доступ для зарегистрированных пользователей
Л1.9	Голембиовская, О. М., Рытов, М. Ю., Шинаков, К. Е., Голембиовский, М. М., Кондрашова, Е. В.	Формализация подхода к определению степени ущерба и потенциала нарушителя: монография	Саратов: Вузовское образование, 2024	https://www.iprbookshop.ru/135004.html неограниченный доступ для зарегистрированных пользователей
Л1.10	Целых, А. Н., Котов, Э. М.	Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2023	https://www.iprbookshop.ru/138009.html неограниченный доступ для зарегистрированных пользователей
Л1.11	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
Л1.12	Бутырский Е. Ю., Цехановский В. В., Жукова Н. А., Баймуратов И. Р., Куликов И. А.	Машинное обучение: учебник	Москва: Директ-Медиа, 2023	https://biblioclub.ru/index.php?page=book&id=701807 неограниченный доступ для зарегистрированных пользователей
Л1.13	Годин А. М.	Статистика: учебник	Москва: Дашков и К°, 2023	https://biblioclub.ru/index.php?page=book&id=710971 неограниченный доступ для зарегистрированных пользователей
5.2. Дополнительная литература				
	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562412 неограниченный доступ для зарегистрированных пользователей
Л2.2	Гулак, М. Л., Рытов, М. Ю., Голембиовская, О. М.	Аудит информационной безопасности. Прикладная статистика: учебное пособие	Москва: Ай Пи Ар Медиа, 2020	https://www.iprbookshop.ru/97630.html неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.3	Замятин, А. В.	Интеллектуальный анализ данных: учебное пособие	Томск: Издательский Дом Томского государственного университета, 2020	https://www.iprbookshop.ru/116889.html неограниченный доступ для зарегистрированных пользователей
Л2.4	Колесниченко, О. Ю.	Data Science (наука о данных) в становлении информационного общества: учебное пособие	Москва: Прометей, 2021	https://www.iprbookshop.ru/125600.html неограниченный доступ для зарегистрированных пользователей
Л2.5	Мисиченко Н. Ю., Веретенникова Е. Г., Кудинова Г. Н.	Документоведение: учебное пособие для направлений 10.03.01 «Информационная безопасность», 38.03.02 «Менеджмент»: учебное пособие	Ростов-на-Дону: Издательско-полиграфический комплекс РГЭУ (РИНХ), 2021	https://biblioclub.ru/index.php?page=book&id=685541 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Консультант+ https://www.cosultant.ru/
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
Google Collab

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-3: способен проводить анализ информационной безопасности объектов и автоматизированных систем на соответствие требованиям стандартов в области информационной безопасности			
З - стандарты информационной безопасности, методы оценки и аудита, основные угрозы и уязвимости, а также принципы интеграции методов защиты в бизнес-процессы и документирования политик безопасности	Демонстрирует понимание особенностей различных стандартов информационной безопасности и сферы их применения для осуществления информационно-аналитической деятельности; идентифицирует угрозы и уязвимости, называет критерии оценки документации информационной безопасности установленным стандартам и требованиям 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	Опрос (вопросы 1-72) Вопросы к зачету (1-24)
У - проводить анализ и аудит информационных систем, выявлять и оценивать риски информационной безопасности	Осуществляет оценку рисков и угроз информационной безопасности, анализ информационной системы с использованием инструментов для выявления уязвимостей, формулирует выводы на основе проведенного анализа и предлагать конкретные меры по устранению выявленных рисков в процессе выполнения практико-ориентированного и задания к зачету	Полнота и содержательность выполненного практико-ориентированного задания; обоснованность обращения к профессиональным базам;	Практико-ориентированные задания (задания 1-16) Задание к зачету
В – навыками подготовки аналитических отчетов и документации с рекомендациями по улучшению информационной безопасности	Формирует структурированные отчеты об аудите информационной безопасности и оценке рисков, отражающие результаты и рекомендации проведенного исследования в процессе выполнения практико-ориентированного и задания к зачету	Полнота и содержательность выполненного практико-ориентированного задания, глубина анализа; использование различных источников информации Интернет ресурсов, в целях осуществления определенных этапов информационно-аналитической деятельности;	Практико-ориентированные задания (задания 1-16) Задание 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

Введение в информационно-аналитическую деятельность. Этапы аналитического исследования. Задачи аналитиков информационной безопасности. Информационно-аналитические системы. Источники и типы данных, генерируемых в информационно-аналитических системах

1. Алгоритм решения аналитических задач.
2. Определение проблемы, постановка, цели, задач и гипотез исследования.
3. Методы статистической обработки, анализа и прогнозирования: идентификация источников информации, сбор данных, предварительная обработка данных
4. Методы статистической обработки, анализа и прогнозирования: анализ данных с помощью методов статистики;
5. Методы статистической обработки, анализа и прогнозирования: простейшие методы моделирования и прогнозирования.
6. Мониторинг информационной безопасности: основные аспекты, этапы и направления.
7. Идентификация рисков информационной безопасности
8. Оценка рисков информационной безопасности
9. Управление рисками информационной безопасности
10. Экономическое обеспечение информационной безопасности: расчет и анализ финансовых показателей, связанных с защитой информации и активов организации
11. Экономическое обеспечение информационной безопасности: обоснование затрат на безопасность
12. Подготовка аналитической и отчетной документации в рамках информационной безопасности.
13. Типы политики, процедур, инструкций, отчетов информационной безопасности.
14. Стандарты информационной безопасности.
15. Аудит и оценка информационной безопасности.
16. Формы и структура аналитических отчетов информационной безопасности.
17. Модель угроз информационной безопасности
18. Типы машинного обучения (с учителем, без учителя, с подкреплением).
19. Алгоритмы машинного обучения (линейная и логистическая регрессия, к-ближайших соседей, деревья решений, случайный лес, к-средних, метод главных компонент, факторный анализ).
20. Метрики качества построенных моделей.
21. Применение методов машинного обучения в информационной безопасности: обнаружение угроз
22. Применение методов машинного обучения в информационной безопасности: анализ поведения пользователей
23. Применение методов машинного обучения в информационной безопасности: защита от фишинга
24. Применение методов машинного обучения в информационной безопасности: обработка естественного языка.

***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.

Задание к зачету

1. Используйте предложенный информационный материал или датасет.
2. Проведите обработку и анализ данных подходящим методом согласно задаче исследования, постройте соответствующие модели
3. Произведите интерпретацию полученных результатов

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 для зачета:

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 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. Что такое информационно-аналитическая деятельность, ее цели и задачи.
2. Значение аналитической деятельности в бизнесе, государственном управлении и других сферах.
3. Необходимые навыки и задачи аналитиков информационной безопасности
4. Этапы аналитического исследования
5. Структура и компоненты информационно-аналитических систем.
6. Обзор существующих информационно-аналитических систем
7. Функциональные возможности аналитических систем: анализ, визуализация, обработка больших данных.
8. Успешные примеры внедрения информационно-аналитических систем в организациях.

9. Типы источников данных: Внутренние (корпоративные базы данных) и внешние (открытые данные, веб-скрейпинг).
10. Структурированные и неструктурированные данные: характеристики и различия между ними.
11. Подходы к сбору данных. Техники и инструменты для сбора информации.
12. Качество данных: как обеспечивается точность и актуальность данных.
13. Вопросы защиты данных и соблюдения законодательства
14. Алгоритм решения аналитических задач.
15. Методология сбора данных. Выбор методов (опросы, интервью, онлайн-формы, автоматизированный сбор данных). Разработка инструментов сбора данных. Соблюдение правовых норм и стандартов в сборе персональных данных.
16. Предварительная обработка данных: очистка данных (устранение дубликатов, обработка пропусков, проверка на ошибки); преобразование данных (нормализация, стандартные форматы, категоризация и кодирование данных); Визуализация данных (построение графиков и диаграмм для общего понимания структуры данных)
17. Описательная статистика: рассмотрение основных характеристик, данных (среднее, медиана, стандартное отклонение).
18. Корреляционный анализ. Исследование взаимосвязей между переменными с использованием коэффициента корреляции.
19. Тестирование гипотез. Применение t-тестов, ANOVA для проверки статистических гипотез.
20. Регрессионный анализ. Применение линейной или множественной регрессии для моделирования зависимостей между переменными.
21. Анализ временных рядов. Методы, такие как скользящее среднее и ARIMA, для прогнозирования на основе исторических данных.
22. Основные аспекты и этапы мониторинга информационной безопасности
23. Применение SIEM-систем и их интеграция с другими инструментами безопасности.
24. Подготовка к мониторингу: определение ресурсов (сервера, сети), которые требуют мониторинга. Разработка плана мониторинга и выбор инструментов.
25. Сбор данных. Методы сбора данных о событиях безопасности, трафике сети, активности пользователей.
26. Анализ собранных данных в процессе мониторинга на предмет выявления инцидентов.
27. Использование аналитических отчетов для оценки состояния безопасности.
28. Разработка процедур реагирования на инциденты и на основе данных полученных в процессе мониторинга.
29. Мониторинг сети: Анализ сетевого трафика для обнаружения аномалий и угроз.
30. Мониторинг приложений: Наблюдение за поведением приложений в реальном времени для выявления уязвимостей.
31. Мониторинг пользователей: Отслеживание действий пользователей для предотвращения внутренних угроз.
32. Идентификация рисков информационной безопасности
33. Выявление угроз и уязвимостей: Оценка потенциальных угроз и уязвимостей с использованием методологий (например, OCTAVE, FAIR).
34. Качественные и количественные методы оценки:
35. Приоритизация рисков: Методики для расстановки приоритетов проблем безопасности и выделение ресурсов на их решение.
36. Выбор стратегий управления рисками информационной безопасности. Разработка планов по снижению рисков.
37. Расчет и анализ финансовых показателей эффективности мероприятий информационной безопасности
38. Ключевые показатели эффективности (KPI): определение показателей для оценки результатов мер по безопасности (количество инцидентов, время реакции).
39. Определение всех затрат, связанных с обеспечением безопасности (лицензии, оборудование, обучение).
40. Анализ возврата на инвестиции (ROI) для различных методов и инструментов безопасности.

41. Обоснование затрат на безопасность. Стоимостный анализ рисков. Оценка финансовых последствий инцидентов безопасности для обоснования вложений. Нахождение компромиссов между стоимостью безопасности и допустимыми рисками.
42. Разработка бюджета на безопасность. Создание обоснованного бюджета на мероприятия по безопасности, включая постоянные и одноразовые расходы.
43. Для глубокого понимания темы подготовки аналитической и отчетной документации в сфере информационной безопасности, вы можете рассмотреть следующие ключевые аспекты и направления изучения:
44. Типы документации информационной безопасности. Определение, назначение и важность политик в организации. Примеры политик информационной безопасности: политика управления доступом, политика управления инцидентами, политика резервного копирования.
45. Примеры процедур: процедуры реагирования на инциденты, процедуры оценки рисков.
46. Примеры инструкций: инструкции по использованию ПО, инструкции по работе с конфиденциальной информацией.
47. Форматы и содержание отчетов, включая аналитические отчеты, отчеты об инцидентах, отчеты о соблюдении политик.
48. Стандарты информационной безопасности
49. Процессы аудита информационной безопасности. Методологии аудита: различные подходами к аудиту безопасности (например, внутренний и внешний аудит).
50. Как оценивать соблюдение политик и процедур, используя чек-листы и контрольные списки.
51. Как оформлять результаты аудита информационной безопасности и рекомендации по улучшению.
52. Формы и структура аналитических отчетов по информационной безопасности.
53. Определение моделей угроз. Понимание концепции и цели моделей угроз в контексте защиты информации.
54. Классификация угроз информационной безопасности.
55. Изучение методов машинного обучения в информационной безопасности — это комплексная задача, охватывающая как теоретические, так и практические аспекты. Для полного понимания этой темы стоит рассмотреть вопросы, связанные с типами и алгоритмами машинного обучения, метриками оценки моделей, а также применением этих методов в различных областях информационной безопасности. Вот подробное руководство по ключевым вопросам для изучения:
56. Типы машинного обучения
57. Алгоритмы машинного обучения
58. Линейная и логистическая регрессия. Как работают линейная и логистическая регрессия? Когда их следует применять? Как интерпретировать коэффициенты регрессии?
59. К-ближайших соседей (k-NN). Как работает алгоритм k-NN и в каких ситуациях он эффективен? Как выбрать значение k и оптимизировать алгоритм?
60. Деревья решений. Углубленное понимание построения деревьев решений: критерии разделения, переобучение и как с ним справляться (например, с помощью обрезки).
61. Случайный лес. Понимание ансамблевых методов: как случайный лес комбинирует деревья решений для улучшения точности и устойчивости моделей.
62. К-средних. Как работает алгоритм к-средних? Применение для кластеризации данных. Как интерпретировать полученные кластеры?
63. Метод главных компонент (PCA) и факторный анализ. Как эти методы помогают в уменьшении размерности данных? Как они могут использоваться для предварительной обработки данных в задачах информационной безопасности?
64. Метрики качества построенных моделей. Точность (Accuracy). F1-мера. ROC и AUC:
65. Кросс-валидация. Зачем нужна кросс-валидация? Как внедрить её в процесс оценки моделей?
66. Методы машинного обучения для обнаружения вредоносного ПО. Как можно использовать алгоритмы для классификации вредоносных программ на основе их поведения или сигнатур?
67. Системы обнаружения вторжений (IDS). Как технологии машинного обучения могут улучшить классификацию и обнаружение аномалий в сетевом трафике?
68. Анализ поведения пользователей. Создание профилей поведения. Как модели могут использоваться для моделирования нормального поведения пользователей и выявления аномалий?

69. Внутренние угрозы. Как машинное обучение помогает обнаруживать потенциальные внутренние угрозы через анализ действий сотрудников?
70. Защита от фишинга. Фильтрация контента. Как можно использовать машинное обучение для автоматической фильтрации фишинговых писем и сайтов? Оценка URL. Методы анализа ссылок и их характеристик для определения вероятности фишинга.
71. Обработка естественного языка (NLP). Анализ текстов. Как NLP может быть использован для анализа текстовых данных на наличие угроз (например, утечек данных, спама)?
72. Классификация документов. Применение машинного обучения для автоматической классификации текстов и анализа ссылок, связанных с киберугрозами.

Критерии оценивания

Максимальный балл – 20.
Число вопросов - 20. 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. Произвести анализ инцидентов информационной безопасности на основе данных отчетов, предоставленных лабораторией Касперского за два года:
1. Изучить оба отчета и выделить ключевые моменты, касающиеся инцидентов информационной безопасности.
2. Сравнить тенденции: определить изменения в типах и количестве инцидентов между двумя отчетами; какие типы атак стали более распространенными? Есть ли снижение или рост числа инцидентов определенного типа? Каковы общие статистические данные (например, количество атак, географическая распространенность, затраты на восстановление)?
3. Рассмотреть и описать последствия выявленных инцидентов для организаций и пользователей.
4. На основе анализа предложите рекомендации для организаций по минимизации риска инцидентов в будущем.
5. Каковы возможные направления для дальнейшего исследования и мониторинга угроз в области информационной безопасности?

Задание 2. Имеются данные о числе инцидентов информационной безопасности в компании за месяц:
27, 82, 18, 42, 25, 73, 67, 70, 93, 58, 36, 22, 72, 13, 59, 65, 87, 10, 99, 67, 44, 39, 85, 23, 50, 13, 12, 13, 93, 79
Необходимо рассчитать среднее число инцидентов, моду, медиану, стандартное отклонение, коэффициент вариации. Сделать выводы.

Задание 3. Имеются данные о числе инцидентов информационной безопасности и ущербе компании от их реализации за месяц

Ущерб, тыс. рублей	27	82	18	42	25	73	67	70	93	58
Число инцидентов	3	8	2	4	2	7	6	7	9	6

Рассчитать среднюю величину ущерба от реализации инцидентов информационной безопасности, стандартное отклонение, коэффициент вариации. Сделать выводы

Задание 4. Имеются данные об инцидентах информационной безопасности в трех регионах за месяц:

Регионы	Общее число инцидентов	Число выявленных уязвимостей	Время реагирования на инциденты	Доля информационных систем, соответствующая стандартам безопасности

Регион 1	120	90	10	96
Регион 2	80	50	15	90
Регион 3	70	60	5	95

Произвести ранжирование регионов по уровню информационной безопасности

Задание 5. Имеются следующие данных по 12 компаниям

Компания	Число инцидентов, ед.	Уровень соответствия стандартам, %	Время реагирования, минут	Уровень уязвимости, %
1	63	97	1,13	51
2	96	63	4,45	29
3	73	75	12,7	77
4	25	92	17,7	73
5	37	95	9,3	35
6	40	89	3,7	47
7	47	93	12,1	58
8	29	55	9,3	24
9	22	85	3,5	60
10	81	71	21,7	77
11	60	65	15,5	69
12	15	74	3,1	77

Выявить возможные взаимосвязи рассматриваемых показателей с помощью коэффициентов корреляции Пирсона и Спирмена.

Задание 6. Имеются квартальные данные о числе инцидентов информационной безопасности на предприятии за несколько лет

Период		2018:3	97	2021:2	128
2016:1	90	2018:4	90	2021:3	125
2016:2	87	2019:1	115	2021:4	130
2016:3	93	2019:2	110	2022:1	145
2016:4	90	2019:3	120	2022:2	140
2017:1	100	2019:4	117	2022:3	137
2017:2	95	2020:1	130	2022:4	140

2017:3	98	2020:2	125	2023:1	147
2017:4	100	2020:3	127	2023:2	140
2018:1	120	2020:4	120	2023:3	143
2018:2	110	2021:1	131	2023:4	145

Рассчитайте темпы роста (цепные и базисные). Постройте аддитивную и мультипликативные модели временного ряда, последовательно выделив сезонную, трендовую и случайную компоненты. Оцените качество аддитивной и мультипликативной моделей. Выберите из них наилучшую.

Задание 7. Идентификация активов предприятия для определения необходимости и целесообразности создания системы защиты.

1. Идентификация бизнес-процессов предприятия.
2. Оценка важности бизнес-процессов
3. Оценка влияния основных компонент ИТ-инфраструктуры
4. Оценка влияния ИТ-компонент на бизнес-процессы
5. Категорирование активов предприятия
6. Необходимость и целесообразность защиты активов
7. Вывод по практическому заданию.

Задание 8. Определение и оценка базовых рисков ИБ идентифицированных активов предприятия

1. Определение необходимости и целесообразности защиты активов предприятия
2. Идентификация существующих мер защиты на предприятии
3. Оценка уязвимости активов для перечня угроз
4. Оценка вероятности реализации угроз
5. Определение базового риска ИБ
6. Вывод по практическому заданию.

Задание 9. Формирование обоснования выбора дополнительных мер защиты с учетом оценки базовых рисков ИБ идентифицированных активов предприятия

1. Определение базовых рисков для активов
2. Методика выбора дополнительных мер защиты
3. Определение остаточных рисков для активов
4. Сопоставление оценок базового и остаточного риска
5. Сопоставление количества УБИ, которые могут быть успешно обработаны на уровне оценок базового риска, до приемлемого уровня остаточного риска
6. Сопоставление оценок базового риска, уровня остаточного риска при выборе различных вариантов выбора мер защиты
7. Расчеты вариантов применения дополнительных мер защиты
8. Вывод по практическому заданию.

Задание 10. Формирование экономического обоснования выбора дополнительных мер защиты с учетом оценки базовых рисков ИБ идентифицированных активов предприятия.

1. Переоценка базовых рисков для активов предприятия по вариантам
2. Модель выбора наиболее экономически оптимального варианта
3. Расчеты NPV для вариантов применения дополнительных мер защиты
4. Определение оптимального варианта по критерию NPV
5. Вывод по практическому заданию.

Задание 11. Составление модели угроз информационной безопасности.

1. Выберите конкретный информационный ресурс для анализа (например, веб-сайт, информационную систему, базу данных и т.д.). Убедитесь, что у вас достаточно информации о выбранном объекте.

2. Используя методы анализа угроз, составьте список возможных угроз, с которыми может столкнуться ваш объект. Рассмотрите, как внутренние, так и внешние угрозы (например, хакерские атаки, утечка данных, внутренние злоупотребления и т.д.).
3. Классифицируйте угрозы по категориям (например, физические, логические, процедурные).
4. Произведите оценку вероятности возникновения каждой угрозы и их потенциального воздействия на информационный ресурс, используя шкалу оценки (например, низкий, средний, высокий).
5. На основе проведенного анализа создайте модель угроз для выбранного информационного ресурса. Вы можете представить её в виде таблицы или схемы, содержащей: перечень угроз, оценку их вероятности, оценку воздействия, предлагаемые меры защиты
6. Напишите выводы по выполненной работе, указав на наиболее критические угрозы и предложенные стратегии защиты.

Задание 12. «Основные положения регрессионного анализа»
Цель: ознакомится с регрессионными методами в машинном обучении.
Задание выполняется в Google Colab
Используйте предложенный датасет.
1. Откройте блокнот с примером по данной теме.
2. Выполните задание по алгоритму, указанному в блокноте.
3. Сделайте выводы.

Задание 13. «Кластеризация»
Цель: ознакомиться с методом кластеризации в машинном обучении.
Задание выполняется в Google Colab
Используйте предложенный датасет.
1. Откройте блокнот с примером по данной теме.
2. Выполните задание по алгоритму, указанному в блокноте.
3. Сделайте выводы.

Задание 14. «Уменьшение размерности»
Цель: ознакомиться с методоми уменьшения размерности в машинном обучении.
Задание выполняется в Google Colab
Используйте предложенный датасет.
1. Откройте блокнот с примером по данной теме.
2. Выполните задание по алгоритму, указанному в блокноте.
3. Сделайте выводы.

Задание 15. «Выявление аномалий»
Цель: ознакомиться с методами машинного обучения по выявлению аномалий в рамках информационной безопасности
Задание выполняется в Google Colab
Используйте предложенный датасет.
1. Откройте блокнот с примером по данной теме.
2. Выполните задание по алгоритму, указанному в блокноте.
3. Сделайте выводы.

Задание 16. «Обработка естественного языка»
Цель: ознакомиться с методами обработки естественного языка в рамках информационной безопасности
Задание выполняется в Google Colab
Используйте предложенный датасет.
1. Откройте блокнот с примером по данной теме.
2. Выполните задание по алгоритму, указанному в блокноте.
3. Сделайте выводы.

Критерии оценивания отдельного практико-ориентированного задания:

Каждое практико-ориентированное задание оценивается максимально по 5 баллов каждое. Максимальное количество баллов за выполнение всех практико-ориентированных заданий – 80 баллов.

- 5 баллов выставляется, если обучающийся: выполнил задание в полном объеме, самостоятельно, с соблюдением необходимой последовательности; грамотно оформил представленный отчет;
- 4 балла 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;
- 2-3 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;
- 0-1 балл 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 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.