Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ И МЕТОДЫ ДЕЛОВОЙ РАЗВЕДКИ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
4	2	72	6	24	0		42	0	3
Итого	2	72	6	24	0	16	42	0	

АННОТАЦИЯ

Цель дисциплины: Формирование у магистрантов системных знаний и практических навыков в области применения информационно-аналитических систем (ИАС) и методов деловой разведки (Business Intelligence, BI) для решения задач обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ), включая прогнозирование, выявление и нейтрализацию киберугроз и рисков.

Задачи дисциплины:

1. Изучить теоретические основы, архитектуру и классификацию современных информационно-аналитических систем и систем деловой разведки.

2. Освоить методы сбора, обработки, анализа и визуализации данных из открытых и внутренних источников для целей безопасности.

3. Сформировать навыки применения методов и инструментов деловой разведки для анализа конкурентной среды, оценки рисков и выявления потенциальных угроз объектам КИИ.

4. Научить проводить аналитическую обработку больших данных (Big Data) для выявления аномалий, паттернов кибератак и прогнозирования инцидентов информационной безопасности.

5. Развить умение разрабатывать предложения по интеграции ИАС и BI-решений в комплексные системы безопасности объектов КИИ.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины: Формирование у магистрантов системных знаний и практических навыков в области применения информационно-аналитических систем (ИАС) и методов деловой разведки (Business Intelligence, BI) для решения задач обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ), включая прогнозирование, выявление и нейтрализацию киберугроз и рисков.

Задачи дисциплины:

1. Изучить теоретические основы, архитектуру и классификацию современных информационно-аналитических систем и систем деловой разведки.

2. Освоить методы сбора, обработки, анализа и визуализации данных из открытых и внутренних источников для целей безопасности.

3. Сформировать навыки применения методов и инструментов деловой разведки для анализа конкурентной среды, оценки рисков и выявления потенциальных угроз объектам КИИ.

4. Научить проводить аналитическую обработку больших данных (Big Data) для выявления аномалий, паттернов кибератак и прогнозирования инцидентов информационной безопасности.

5. Развить умение разрабатывать предложения по интеграции ИАС и BI-решений в комплексные системы безопасности объектов КИИ.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина "Информационно-аналитические системы и методы деловой разведки" относится к вариативной части образовательной программы.

Она логически связана с дисциплинами:

• Предшествующие: "Системы защиты информации на объектах КИИ", "Управление информационными рисками", "Теория информации и кодирования".

• Сопутствующие: "Криптографические методы защиты информации", "Организационно-правовое обеспечение информационной безопасности".

• Последующие: Является основой для прохождения производственной практики и выполнения магистерской диссертации, в части, связанной с аналитическим обоснованием предлагаемых решений.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**

Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
научно-исследовательский			
Анализ фундаментальных и прикладных проблем ИБ в условиях становления современного информационного общества; выполнение научных исследований в области ИБ; подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях	Фундаментальные и прикладные проблемы информационной безопасности; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.030	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем

			защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	4 Семестр						
1	Теоретические основы и инструменты деловой разведки и аналитики	1-8	4/12/0		25	КИ-8	З-ПК-3, У-ПК-3, В-ПК-3
2	Применение информационных	9-15	2/12/0		25	КИ-15	З-ПК-3, У-ПК-3,

	аналитических систем и мотодов деловой разведки для защиты объектов КИИ						В-ПК-3
	Итого за 4 Семестр		6/24/0		50		
	Контрольные мероприятия за 4 Семестр				50	З	З-ПК-3, У-ПК-3, В-ПК-3

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	4 Семестр	6	24	0
1-8	**Теоретические основы и инструменты деловой разведки и аналитики**	4	12	0
1	**Введение в дисциплину.** Введение в дисциплину. Цели, задачи курса. Базовые понятия: BI, ИАС, их роль в защите КИИ. Связь с профессиональными обязанностями. Понятия деловой разведки (BI), информационно-аналитических систем (ИАС). Роль и место в системе безопасности объектов КИИ.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
2	**Тема 1.Источники информации для деловой разведки. Часть 1.** Классификация источников (OPEN/OSINT, CLOSED). Юридические и этические рамки сбора данных. Источники информации для деловой разведки. Классификация источников (открытые, полуоткрытые, закрытые).	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
3	**Тема 2. Источники информации для деловой разведки. Часть 2.** Юридические и этические аспекты сбора информации. Методы OSINT.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
4	**Тема 3. Архитектура и компоненты современных ИАС и BI-платформ. Часть 1.** Ключевые компоненты: ETL, Хранилища данных, средства анализа и визуализации. Понятие OLAP-кубов.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
5	**Тема 4. Архитектура и компоненты современных ИАС и BI-платформ.** ETL-процессы, хранилища данных (Data Warehouse),	Всего аудиторных часов		
		0	2	0
		Онлайн		

	витрины данных (Data Mart).	0	0	0
6	**Тема 5. Методы анализа данных. Часть 1.** От дескриптивной статистики к предиктивной аналитике. Введение в Data Mining (кластеризация, классификация).	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
7	**Тема 6. Методы анализа данных. Часть 2.** Дескриптивный, диагностический, предиктивный и предписывающий анализ. Введение в Data Mining.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
8	**Тема 7. Анализ социальных сетей (SNA).** Сформировать у студентов практические навыки анализа социальных сетей для выявления скрытых связей, сообществ и ключевых фигур, представляющих потенциальный интерес с точки зрения безопасности объекта КИИ. Введение в SNA: Что такое анализ социальных сетей и как он применяется в контексте безопасности и деловой разведки. Ключевые метрики: Объяснение базовых понятий SNA: "центральность" (выявление ключевых influencers), "плотность связей", "сообщества".	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
9-15	**Применение информационных аналитических систем и мотодов деловой разведки для защиты объектов КИИ**	2	12	0
9	**BI в системе управления киберрисками.** Корреляция событий ИБ, системы класса SIEM как частный случай ИАС.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
10	**BI в системе управления киберрисками.** Корреляция событий ИБ, системы класса SIEM как частный случай ИАС.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
11	**Предиктивная аналитика в информационной безопасности.** Прогнозирование инцидентов на основе исторических данных. Методы машинного обучения для обнаружения аномалий.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
12	**Предиктивная аналитика в информационной безопасности.** Прогнозирование инцидентов на основе исторических данных. Методы машинного обучения для обнаружения аномалий.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
13	**Анализ больших данных (Big Data) для безопасности.** Анализ киберугроз для объектов КИИ. Работа с платформами Threat Intelligence (например, AlienVault OTX). Анализ тактик и методик APT-групп, целевых объектов и используемых уязвимостей.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
14	**Разработка концепции ИАС для объекта КИИ.** Разработка концепции ИАС для объекта КИИ.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
15	**Зачетное занятие. Защита проектов, ответы на вопросы.**	Всего аудиторных часов		
		0	2	0

	Зачетное занятие. Защита проектов, ответы на вопросы.	Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные траектории по курсу

• Базовая траектория: Выполнение всех обязательных практических работ и самостоятельных заданий в срок, активная работа на семинарах.

• Углубленная траектория (проектная): Помимо базовых заданий, выполнение индивидуального или командного проекта по выбору (например, углубленный анализ конкретной Advanced Persistent Threat (APT) группы, targeting объекты КИИ, или разработка прототипа дашборда для конкретного сценария).

• Исследовательская траектория: Написание научной статьи или обзора по актуальной проблеме на стыке BI и ИБ (например, "Применение методов NLP для анализа утечек данных в даркнете") на основе материалов курса.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-3	З-ПК-3	З, КИ-8, КИ-15
	У-ПК-3	З, КИ-8, КИ-15
	В-ПК-3	З, КИ-8, КИ-15

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-

балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-х балльной шкале</th><th>Отметка о зачете</th><th>Оценка ECTS</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td rowspan="7">«Зачтено»</td><td>A</td></tr>
<tr><td>85-89</td><td rowspan="2">4 – «хорошо»</td><td>B</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>«Не зачтено»</td><td>F</td></tr>
</table>

Оценка «отлично» соответствует глубокому и прочному освоению материала программы обучающимся, который последовательно, четко и логически стройно излагает свои ответы, умеет тесно увязывать теорию с практикой, использует в ответах материалы монографической литературы.

Оценка «хорошо» соответствует твердым знаниям материала обучающимся, который грамотно и, по существу, излагает свои ответы, не допуская существенных неточностей.

Оценка «удовлетворительно» соответствует базовому уровню освоения материала обучающимся, при котором освоен основной материал, но не усвоены его детали, в ответах присутствуют неточности, недостаточно правильные формулировки, нарушения логической последовательности.

Отметка «зачтено» соответствует, как минимум, базовому уровню освоения материала программы, при котором обучающийся владеет необходимыми знаниями, умениями и навыками, умеет применять теоретические положения для решения типовых практических задач.

Оценку «неудовлетворительно» / отметку «не зачтено» получает обучающийся, который не знает значительной части материала программы, допускает в ответах существенные ошибки, не выполнил все обязательные задания, предусмотренные программой. Как правило, такие обучающиеся не могут продолжить обучение без дополнительных занятий.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации и разработки приложений, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой построения измерительных комплексов по анализу защищенности объектов информатизации и проведению инструментальных специальных исследований при аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

Проведение лабораторных работ - не предусмотрено

На практических занятиях выносятся вопросы уровня навыков и умений. Задания выполняются студентами с использованием сети Интернет. На каждом рабочем месте должен быть развернут персональный компьютер (АРМ) с выходом в интернет. Результаты, полученные в ходе практических занятий, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний (разделы 1 и 2) используются контрольные вопросы. Для повышения результатов контроля студентами (по их желанию) могут быть выполнены и использованы письменные работы (рефераты).

В процессе итогового контроля также могут использоваться результаты, полученные студентами на практических занятиях.

Для успешного освоения курса необходимы базовые знания в области информационной безопасности, сетевых технологий и основ программирования.

Акцент в курсе делается на практическое применение знаний. Посещение лекций даст теоретический фундамент, но ключевые навыки формируются на практических занятиях.

Используйте предоставленные материалы и рекомендованное программное обеспечение. Большинство современных BI-инструментов имеют бесплатные версии или trial-периоды.

При выполнении OSINT-заданий строго соблюдайте законодательство и этические нормы. Все задания выполняются в учебных целях на условных или публично доступных данных.

Начинайте работу над самостоятельными заданиями заранее, они требуют системного подхода и анализа большого объема информации.

Для проектной работы формируйте команды с учетом разнообразия навыков (аналитики, визуализаторы, предметные эксперты).

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса «Конкурентная разведка и информационное противоборство», практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Курс носит прикладной характер. Лекционный материал должен подкрепляться реальными кейсами из практики обеспечения безопасности объектов КИИ.

Рекомендуется приглашать для проведения гостевых лекций практиков из сферы ИБ и BI.

На практических занятиях целесообразно использовать метод проектного обучения, когда студенты работают над сквозной задачей на протяжении всего курса.

Важно создавать в аудитории атмосферу, приближенную к реальной работе аналитика: постановка нечетких задач, работа с "зашумленными" данными, необходимость самостоятельно выбирать инструменты и методы анализа.

При оценке проектов следует учитывать не только техническую корректность, но и обоснованность выбранных подходов, ясность представления результатов и умение отвечать на вопросы по проекту.

Необходимо обеспечить всех студентов доступом к необходимым программным платформам (виртуальные лаборатории, облачные сервисы с академическими лицензиями).

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы – «Обеспечение безопасности значимых объектов критической информационной инфраструктуры», место курса в различных областях науки и техники.

В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

КЛР8, КЛР15 - максим. балл-25, мин. балл – 15. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.При неаттестации хотя бы по одному из разделов, студент не допускается к зачёту.

Автор(ы):

Дворянкин Сергей Владимирович, д.т.н., профессор