МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» ____02____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Аналитика информационной безопасности»

Направление подготовки/специальность
09.03.03 Прикладная информатика

Профиль/специализация
«Информационные технологии управления бизнесом»

Квалификация
бакалавр

Формы обучения
очная

Москва, 2023 г.

Разработчик(и):

ст.преподаватель / М.В.Даньшина/

Согласовано:
Заведующий кафедрой «Инфокогнитивные технологии»,
к.т.н., доцент / Е.А. Пухова /

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К основным целям освоения дисциплины «Аналитика информационной безопасности» следует отнести:

- Формирование навыков у студентов, необходимых для поиска активных угроз, формирования полного представления о происходящем, а в результате придумать ответ и заблокировать эти угрозы.

К основным задачам освоения дисциплины «Аналитика информационной безопасности» следует отнести:

- Изучить типы анализа информационной безопасности;
- Выделять конкретные события, на которых будет идти сосредоточение;
- Оперативно разрабатывать решения для ответа на активные угрозы.

Обучение по дисциплине «Аналитика информационной безопасности» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИОПК-3.1. Знает принципы информационной и библиографической культуры, методы, способы и средства получения, хранения и переработки информации; принципы построения современных информационно-коммуникационных технологий; модели организации данных, сетевые модели, иерархические модели, реляционную модель и объектную модель. ИОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ИОПК-3.3. Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к числу учебных дисциплин части, формируемой участниками образовательных отношений.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП:

Базы данных;
Разработка КИС;
Администрирование серверов;
Веб разработка.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часа).

3.1 Виды учебной работы и трудоемкость для очной формы обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			7	
1	**Аудиторные занятия**	**72**	72	
	В том числе:			
1.1	Лекции	8	8	
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	64	64	
2	**Самостоятельная работа**	**72**	72	
3	**Промежуточная аттестация**			
	Экзамен		экзамен	
	Итого:	**144**	144	

3.2 Тематический план изучения дисциплины для очной формы обучения

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/практические занятия	Лабораторные занятия	Практическая подготовка	
1	Введение в информационно-аналитическую деятельность	7	1		2		4
2	Технологический цикл ИАДКБ	7	1		2		4
3	Первичная обработка информации	7	1		2		4
4	Методика информационного поиска	7	1		2		4
5	Основные принципы аналитической деятельности	9	1		4		4
6	Планирование ИАДКБ. Этапы ИАДКБ. Системный подход в ИАДКБ	9	1		4		4
7	Анализ информативности источников	9	1		4		4

8	Оценка полноты, непротиворечивости и достоверности информации. Технология создания аналитических документов	9	1		4		4
9	Отчетные документы ИАДКБ. Заключение	8			4		4
10	Система информационно-аналитического обеспечения в сфере безопасности	8			4		4
11	Информационно-аналитические центры в РФ, их функции	8			4		4
12	Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности	8			4		4
13	Информационно-аналитическое обеспечение деятельности МВД в сфере компьютерных преступлений	8			4		4
14	Анализ современного состояния «хакерства» в России и за рубежом	8			4		4
15	Информационно-аналитическая работа в команде	8			4		4
16	Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности	8			4		4
17	Анализ современного состояния «хакерства» в России и за рубежом	8			4		4
18	Информационно-аналитическая работа в команде	8			4		4
Итого		**144**	**8**		**64**		**72**

3.3 Содержание дисциплины

Введение в информационно- аналитическую деятельность

Технологический цикл ИАДКБ

Первичная обработка информации

Методика информационного поиска

Основные принципы аналитической деятельности

Планирование ИАДКБ. Этапы ИАДКБ. Системный подход в ИАДКБ

Анализ информативности источников

Оценка полноты, непротиворечивости и достоверности информации. Технология создания аналитических документов

Отчетные документы ИАДКБ. Заключение

Система информационно-аналитического обеспечения в сфере безопасности

Информационно-аналитические центры в РФ, их функции

Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности

Информационно-аналитическое обеспечение деятельности МВД в сфере компьютерных преступлений

Анализ современного состояния «хакерства» в России и за рубежом

Информационно-аналитическая работа в команде

Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности

Анализ современного состояния «хакерства» в России и за рубежом

Информационно-аналитическая работа в команде

3.4 Тематика лабораторных занятий

Введение в информационно- аналитическую деятельность

Технологический цикл ИАДКБ

Первичная обработка информации

Методика информационного поиска

Основные принципы аналитической деятельности

Планирование ИАДКБ. Этапы ИАДКБ. Системный подход в ИАДКБ

Анализ информативности источников

Оценка полноты, непротиворечивости и достоверности информации. Технология создания аналитических документов

Отчетные документы ИАДКБ. Заключение

Система информационно-аналитического обеспечения в сфере безопасности

Информационно-аналитические центры в РФ, их функции

Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности

Информационно-аналитическое обеспечение деятельности МВД в сфере компьютерных преступлений

Анализ современного состояния «хакерства» в России и за рубежом

Информационно-аналитическая работа в команде

Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности

Анализ современного состояния «хакерства» в России и за рубежом

Информационно-аналитическая работа в команде

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);

2. Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика, утвержденный приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 922.

3. Приказ Министерства образования и науки РФ от 05 апреля 2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры;

4. Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утвержденный приказом Минобрнауки России от 29 июня 2015 г. № 636;

5. Положение о практической подготовке обучающихся, утвержденное приказом Министерства науки и высшего образования Российской Федерации и Министерства просвещения Российской Федерации от 5 августа 2020 г. № 885/390.

4.2 Основная литература

Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 324 с. — ISBN 978-5-507-48149-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/341267 (дата обращения: 27.09.2023). — Режим доступа: для авториз. пользователей.

4.3 Дополнительная литература

Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242 (дата обращения: 27.09.2023). — Режим доступа: для авториз. пользователей.

4.4 Электронные образовательные ресурсы

https://online.mospolytech.ru/enrol/index.php?id=12335

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Браузеры Chrome, Edge, Firefox
2. OpenVPN с правами для запуска у студентов
3. FileZilla
4. PuTTy
5. Python 3.10
6. Wireshark

4.6 Современные профессиональные базы данных и информационные справочные системы

1. https://owasp.org/

5 Материально-техническое обеспечение

Для проведения лабораторных работ и самостоятельной работы студентов подходят аудитории, оснащенные компьютерами с программным обеспечением в соответствии со списком в пункте 4.5 и подключенные к интернету.

Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов.

Рабочее место преподавателя должно быть оснащено компьютером с подключенным к нему проектором или иным аналогичным по функциональному назначению оборудованием.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции и самостоятельная работа.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к промежуточной аттестации, а также самостоятельно изучают отдельные темы учебной программы.

На занятиях студентов, в том числе предполагающих практическую деятельность, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

Приветствуется обсуждение самих заданий с другими студентами: можно как давать, так и получать советы по общей стратегии выполнения и изучения материала, давать и получать помощь в отладке. Однако писать код студент должен самостоятельно. Делиться кодом или писать его совместно запрещено.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Промежуточная аттестация обучающихся в форме экзамена (д. зачета) проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по

данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания Описание

Отлично Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

Хорошо Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.

Удовлетворительно Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.

Неудовлетворительно Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Текущий контроль

Примерный список вопросов

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

7.3.2 Промежуточная аттестация

1. Особенности архитектуры систем информационно-аналитического обеспечения?
2. Какие функции выполняют центры?
3. Какие отличия полномочий российских и зарубежных центров?
4. Специфика сферы информационной безопасности в контексте аналитической деятельности.
5. Сущность информационно-аналитического обеспечения.
6. Особенности обеспечения розыскных мероприятий в сфере компьютерных преступлений?
7. Отличие хакеров и криптоаналитиков.

8. Общественный вред хакерства.
9. Что такое психологическая совместимость в группах аналитиков?
10. Как организуется команда для «мозгового штурма»?
11. Основные принципы аналитической деятельности.
12. Типы анализов информационной безопасности.
13. Как визуализировать аналитику безопасности?
14. Аналитик информационной безопасности – кто он такой?
15. Перспективы становления информационно-аналитической деятельности в сфере информационной безопасности.
16. Критерии, параметры ограничения логической непротиворечивости и достоверности информации.
17. Проблема активной фильтрации сообщений. Качественные характеристики информации. Режимы восприятия информации. Атрибуция сообщений.
18. Планирование ИАДКБ. Этапы ИАДКБ. Системный подход в ИАДКБ.
19. Понятийный каркас и структурно-функциональная организация информационно-аналитических технологий.
20. Цели, задачи, объект, предмет информационно-аналитической деятельности комплексной безопасности (далее – ИАДКБКБ). Специфика ИАДКБ.
21. Оценка полноты, непротиворечивости и достоверности информации.
22. Технология создания аналитических документов.
23. Алгоритм действий при обнаружении атаки.
24. Алгоритм проведения предпроектных исследований.
25. Алгоритм описания атаки.