МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» 02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Аналитика информационной безопасности»

Направление подготовки
09.03.01 Информатика и вычислительная техника

Профиль
«Кибербезопасность автоматизированных систем»

Квалификация
Бакалавр

Формы обучения
очная

Москва, 2023 г.

Разработчик(и):

степень, звание, должность /_____/

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность», /А.Ю. Гневшев/

Руководитель образовательной программы, /А.Ю. Гневшев/

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

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИУК-1.1. Анализирует задачу, выделяя ее базовые составляющие ИУК-1.2. Осуществляет поиск, критически оценивает, обобщает, систематизирует и ранжирует информацию, требуемую для решения поставленной задачи ИУК-1.3. Рассматривает и предлагает рациональные варианты решения поставленной задачи, используя системный подход, критически оценивает их достоинства и недостатки
ПК-6. Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности	ИПК-6.1. Знает: теоретические основы проектирования крупного масштаба и сложных систем; стандарты оформления технических заданий; методы концептуального, функционального и логического проектирования систем; методы тестирования; международные стандарты на структуру документов требований; нормативные и методические материалы по созданию документов требований к системам; методы оценки качества программных систем; способы масштабирования информационных систем для учета их при логическом проектировании. ИПК-5.2. Умеет: формулировать цели, исходя из анализа проблем, потребностей и возможностей; разрабатывать технико-

	экономическое обоснование; декомпозировать функции на подфункции; алгоритмизировать деятельность; разрабатывать структуры типовых документов; исполнять ручные тесты, проектировать и разрабатывать сложные системы; использовать основные приемы web-дизайна. Внедрять графические, звуковые, анимационные объекты в систему; формировать интерактивные блоки web-ресурса; разрабатывать модели концептуальной, функциональной и логической архитектуры системы; спроектировать информационную систему для заданного предприятия по заданным характеристикам с помощью конфигурирования и программирования. ИПК-5.3. Владеет: навыками концептуального, функционального и логического проектирования; средствами автоматизации проектирования ПО, работы со средствами Internet и Web-технологий для решения задач профессиональной деятельности; навыками проектирования схемы последовательностей, состояний и взаимодействий компонентов системы

2 Место дисциплины в структуре образовательной программы

Дисциплина «Аналитика информационной безопасности» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б1.1) основной образовательной программы (Б1.1.29).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 8 зачетных единиц, т.е. **288** академических часов (лекции – 36 часов, лабораторные занятия – 108 часов, самостоятельная работа - 144 часа), форма контроля – дифференцированный зачёт в 5 семестре, курсовой проект, экзамен в 6 семестре.

Структура и содержание дисциплины «Аналитика информационной безопасности» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость (по очной форме обучения)

№ п/п	Вид учебной работы	Количество часов	Семестры	
			5	6
1	**Аудиторные занятия**	**144**	72	72
	В том числе:			
1.1	Лекции	36	18	18
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	108	54	54
2	**Самостоятельная работа**	144	72	72
3	**Промежуточная аттестация**			
	Дифференцированный зачёт		+	
	Экзамен			+
	Итого:	**288**	144	144

3.2. Тематический план изучения дисциплины (по формам 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	16	2		6		8
2	Технологический цикл ИАДКБ	16	2		6		8
3	Первичная обработка информации	16	2		6		8
4	Методика информационного поиска	16	2		6		8
5	Основные принципы аналитической деятельности	16	2		6		8
6	Планирование ИАДКБ. Этапы ИАДКБ. Системный подход в ИАДКБ	16	2		6		8
7	Анализ информативности источников	16	2		6		8
8	Оценка полноты, непротиворечивости и достоверности информации Технология создания аналитических документов	16	2		6		8
9	Отчетные документы ИАДКБ. Заключение	16	2		6		8
10	Информационно-аналитические центры в РФ, их функции	16	2		6		8
11	Информационно-аналитическое обеспечение деятельности	16	2		6		8

	специалистов сфере информационной безопасности						
12	Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности	16	2		6		8
13	Система информационно-аналитического обеспечения в сфере безопасности	16	2		6		8
14	Анализ современного состояния «хакерства» в России и за рубежом	16	2		6		8
15	Информационно-аналитическая работа в команде	16	2		6		8
16	Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности	16	2		6		8
17	Анализ современного состояния «хакерства» в России и за рубежом	16	2		6		8
18	Информационно-аналитическая работа в команде	16	2		6		8
Итого		**288**	**36**		**108**		**144**

Содержание дисциплины

Раздел 1

Введение в информационно- аналитическую деятельность

Раздел 2

Технологический цикл ИАДКБ

Раздел 3

Первичная обработка информации

Раздел 4

Методика информационного поиска

Раздел 5

Основные принципы аналитической деятельности

Раздел 6

Планирование ИАДКБ. Этапы ИАДКБ. Системный подход в ИАДКБ

Раздел 7

Анализ информативности источников

Раздел 8

Оценка полноты, непротиворечивости и достоверности информации
Технология создания аналитических документов

Раздел 9

Отчетные документы ИАДКБ. Заключение

Раздел 10

Система информационно-аналитического обеспечения в сфере безопасности

Раздел 11

Информационно-аналитические центры в РФ, их функции

Раздел 12

Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности

Раздел 13

Информационно-аналитическое обеспечение деятельности МВД в сфере компьютерных преступлений

Раздел 14

Анализ современного состояния «хакерства» в России и за рубежом

Раздел 15

Информационно-аналитическая работа в команде

Раздел 16

Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности

Раздел 17

Анализ современного состояния «хакерства» в России и за рубежом

Раздел 18

Информационно-аналитическая работа в команде

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997. № 41. стр. 8220-8235.
2. Федеральный закон от 07.08.2001 № 119-ФЗ «Об аудиторской деятельности» // СЗ РФ. 2001. № 33 (часть I).ст. 3422.
3. Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной подписи» // СЗ РФ. 2002. № 2. ст. 127.
4. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. ст. 3283.
5. Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3448.
7. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006.

№ 31 (1 ч.).ст. 3451.

4.2 **Основная литература**

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531084.

2. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. – Санкт-Петербург : Издательство Политехнического университета, 2014. – 322 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 28.08.2019). – ISBN 978-5-7422-4331-1. – Текст : электронный.

3. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2023. — 170 с. — (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/532474.

4. Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. – 4-е изд., стер. – Москва : Флинта, 2016. – 100 с. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93259 (дата обращения: 28.08.2019). – Библиогр.: с. 83-84. – ISBN 978-5-9765-1277-1. – Текст : электронный.

4.3 Дополнительная литература

4.2. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 28.08.2019). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.

https://e.lanbook.com/book/216425

4.3. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=480637 (дата обращения:

28.08.2019). – Библиогр. в кн. – Текст : электронный.
https://reader.lanbook.com/book/306455#8

4.4 Электронные образовательные ресурсы

Электронный образовательный ресурс разрабатывается

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Операционная система Microsoft Windows.
2. Веб-браузер Chrome.

4.6 Современные профессиональные базы данных и информационные справочные системы

1. Федеральная государственная информационная система - Национальная электронная библиотека (НЭБ) https://нэб.рф
2.

5. Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6. Методические рекомендации

6.2. Методические рекомендации для преподавателя по организации обучения

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **09.03.01 «Информатика и вычислительная техника».**

6.3. 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.

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

7. Фонд оценочных средств

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

- экзамен.

Образцы вопросов к экзамену приведены в приложении.

7.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

7.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
ПК-6	Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности

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.

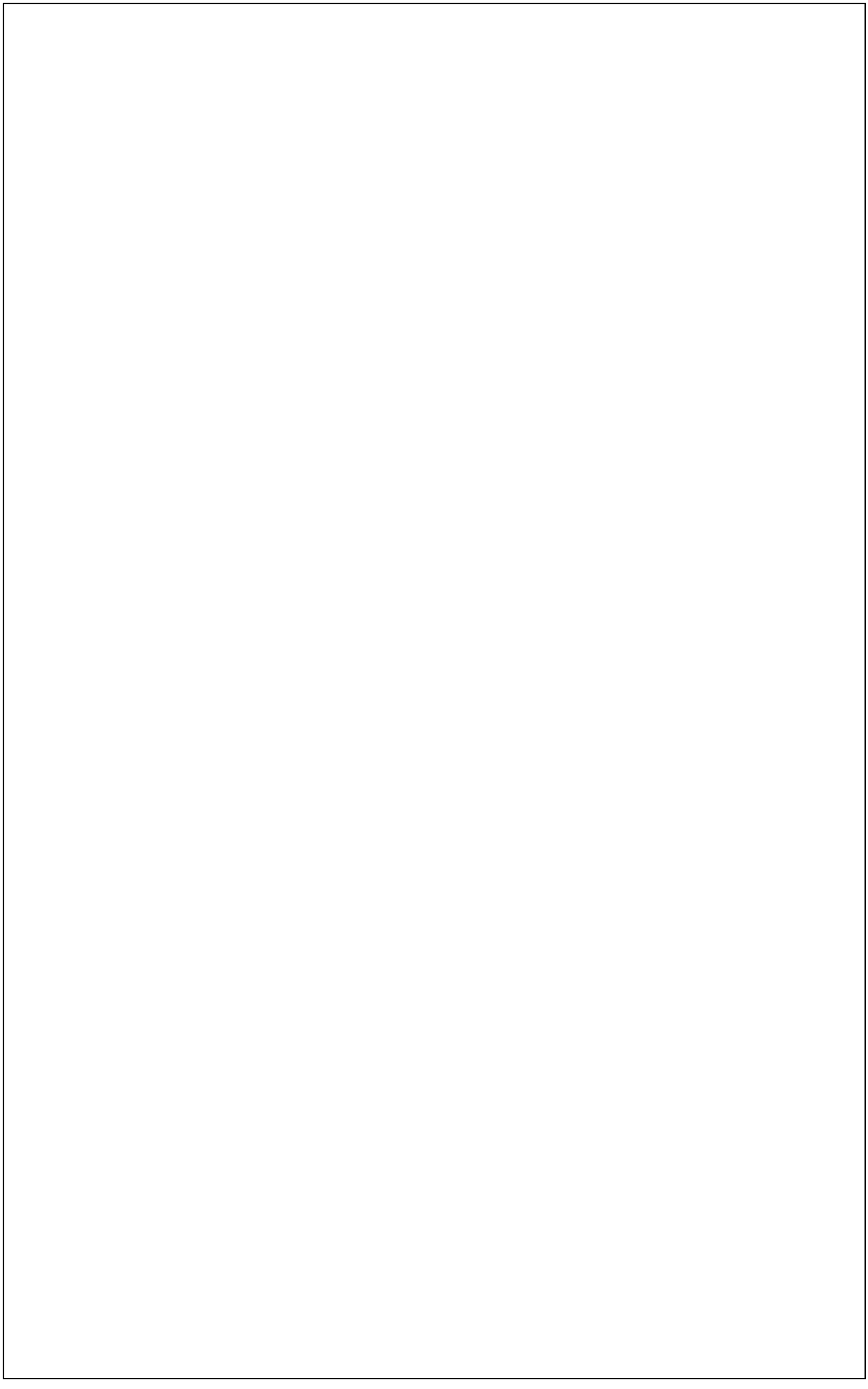
7.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

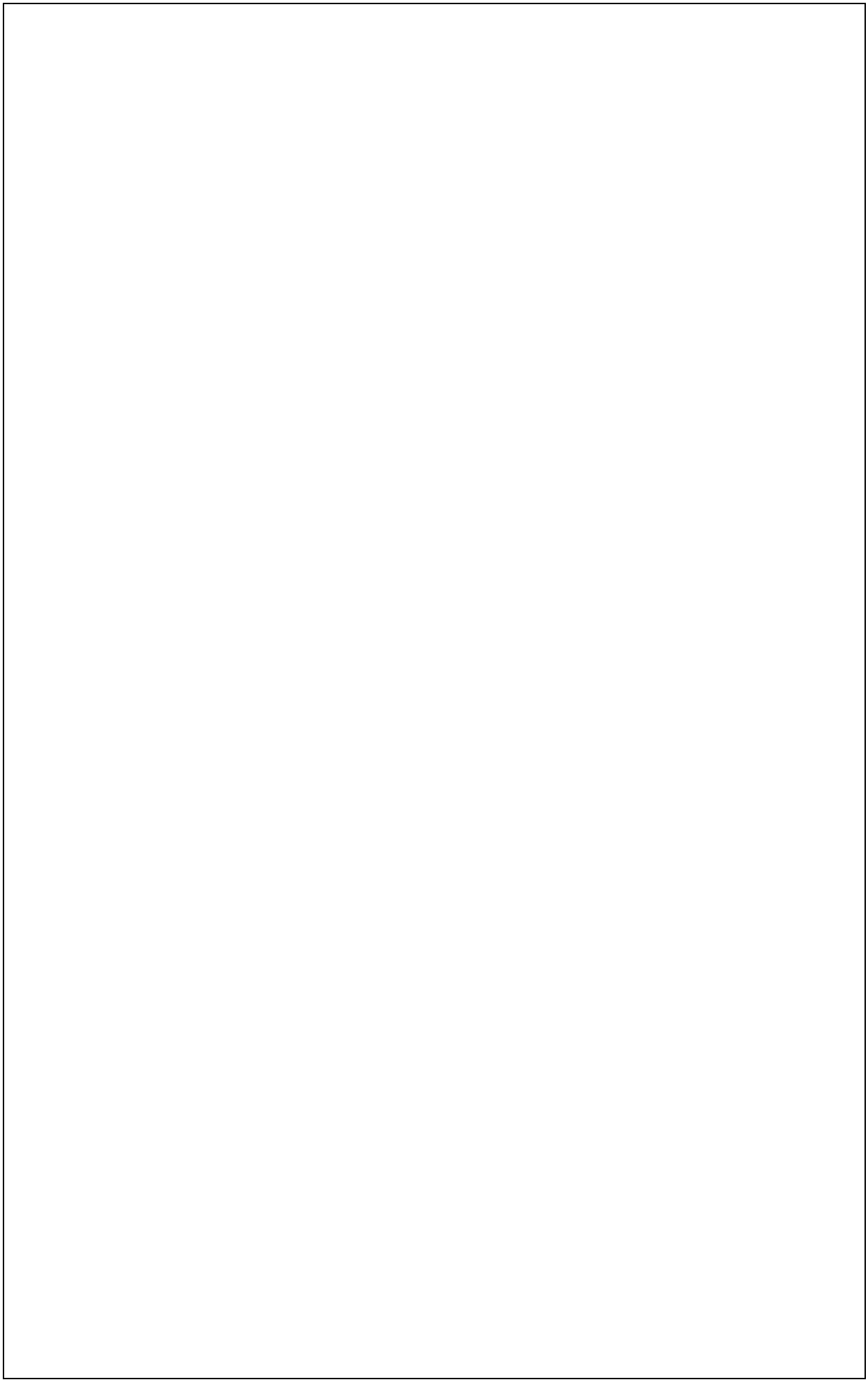
Показатель	Критерии оценивания			
	2	3	4	5
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач				

К-1. Способ обеноосущ е

ствляетьадминистрированиепроцессаконтролляпроизводительно



стисетевыхустройствипрограммногообеспечения,проводитьре



гламентированные работы на сетевых устройствах программно-о

ИУК-1.1. Анализирует задачу, выделяя ее базовые составляющие ИУК-1.2. Осуществляет поиск, критически оценивает, обобщает, систематизирует и ранжирует информацию, требуемую для решения поставленной задачи ИУК-1.3. Рассматривает и предлагает рациональные варианты решения поставленной задачи,	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

используя системный подход, критически оценивает их достоинства и недостатки		значительные затруднения при оперировании знаниями при их переносе на новые ситуации.		
ПК-6. Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности				
ИПК-6.1. Знает: теоретические основы проектирования крупного масштаба и сложных систем; стандарты оформления технических заданий; методы концептуального, функционального и логического проектирования систем; методы тестирования; международные стандарты на структуру документов требований; нормативные и методические материалы по созданию документов требований к системам; методы оценки качества программных систем; способы масштабирования информационных систем для учета их при логическом проектировании. ИПК-5.2. Умеет: формулировать цели, исходя из анализа проблем, потребностей и возможностей; разрабатывать технико-экономическое обоснование; декомпозировать функции на подфункции; алгоритмизировать деятельность; разрабатывать структуры типовых документов; исполнять ручные	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

тесты, проектировать и разрабатывать сложные системы; использовать основные приемы web-дизайна. Внедрять графические, звуковые, анимационные объекты в систему; формировать интерактивные блоки web-ресурса; разрабатывать модели концептуальной, функциональной и логической архитектуры системы; спроектировать информационную систему для заданного предприятия по заданным характеристикам с помощью конфигурирования и программирования. ИПК-5.3. Владеет: навыками концептуального, функционального и логического проектирования; средствами автоматизации проектирования ПО, работы со средствами Internet и Web-технологий для решения задач профессиональной деятельности; навыками проектирования схемы последовательностей, состояний и взаимодействий компонентов системы.				

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: дифференцированный зачет.

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.

Список вопросов для экзамена по дисциплине

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.