Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 13.10.2023 16:40:24
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

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

УТВЕРЖДАЮ
Декан факультета информационных технологий
/Д. Г. Демидов/
«28» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Аналитика информационной безопасности»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчики:

Преподаватель / А.А. Кривоногов /
Преподаватель /А.С. Плоткин/

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	4
2	Место дисциплины в структуре образовательной программы	5
3	Структура и содержание дисциплины	5
3.1	Виды учебной работы и трудоемкость	5
3.2	Тематический план изучения дисциплины	6
3.3	Содержание дисциплины	9
4	Учебно-методическое и информационное обеспечение	13
4.1	Нормативные документы и ГОСТы	13
4.2	Основная литература	14
4.3	Дополнительная литература	14
5	Материально-техническое обеспечение	15
6	Методические рекомендации	15
6.1	Методические рекомендации для преподавателя по организации обучения	15
6.2	Методические указания для обучающихся по освоению дисциплины	15
7	Фонд оценочных средств	16
7.1	Методы контроля и оценивания результатов обучения	16
7.2	Шкала и критерии оценивания результатов обучения	16
7.3	Оценочные средства	19

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**
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ИОПК-8.1. Знает необходимые нормативно-методические документ ИОПК-8.1. Умеет составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем. ИОПК-8.3. Владеет методами
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИОПК-10.1. Знает принципы формирования политики информационной безопасности в информационных системах; ИОПК-10.2. Умеет разрабатывать частные политики информационной безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, управлять процессом их реализации на объекте защиты. ИОПК-10.3. Владеет методами работы технического специалиста и поддержкой выполнения комплекса мер по обеспечению информационной безопасности, управлением процессом их реализации на объекте защиты

ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов	ИОПК-11.3. Владеет навыками проведения физического эксперимента и обработки его результатов, методами расчета и инструментального контроля показателей технической защиты информации.
ПК-6. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ИПК-6.1. Знает принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); ИПК-6.2. владеет методами организации и управления деятельность служб защиты информации на предприятии.

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 (Б1.29).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: Введение в аналитику информационной безопасности.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, т.е. **108** академических часов (лекции – 18 часов, лабораторные занятия – 36 часов, самостоятельная работа - 54 часа), форма контроля – дифференцированный зачёт в 4 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	Семестр
			4
1	**Аудиторные занятия**	**54**	54
	В том числе:		
1.1	Лекции	18	18
1.2	Семинарские/практические занятия		
1.3	Лабораторные занятия	36	36
2	**Самостоятельная работа**	54	54
3	**Промежуточная аттестация**		
	Дифференцированный зачёт		+
	Экзамен		
	Итого:	**108**	108

3.1.1 Очная форма обучения

3.1.2 Очно-заочная форма обучения
Не предусмотрена

3.1.3 Заочная форма обучения
Не предусмотрена

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	Раздел 1.						
1	Тема 1. Введение.		2				4
2	Тема 2. Введение. Аналитическая культура.		3				4
3	Тема 3. Сбор данных. Выбор источников.		2		4		4
4	Тема 4. Качественные навыки специалистов по аналитике данных.				4		4
5	Тема 5. Анализ данных.		2		7		5
6	Тема 6. Оценка деятельности по управлению информационной безопасности.						4
7	Тема 7. Процесс выработки программы получения метрик безопасности.		3				5
8	Тема 8. Измерения информационной безопасности.		2				4
9	Тема 9. Обеспечение информационной безопасности банковских карт.		2				4
10	Тема №10. Основные виды мошенничества с банковскими картами для эквайера.		2				4
11	Тема №11. Исследование банковских карт.				7		4
12	Тема №12. Расследование инцидентов информационной безопасности.				7		4
13	Тема №13. Расследование инцидентов информационной безопасности.				7		4
Итого		**144**	**18**		**36**		**54**

3.2.2 Очно-заочная форма обучения
Не предусмотрена.

3.2.2 Заочная форма обучения
Не предусмотрена

3.2 Содержание дисциплины

Раздел 1
Введение. Понятие Аудита и его виды. Назначение Аудита. Специфика проведения Аудита информационной безопасности организации.
Раздел 2
Тема 2. Введение. Аналитическая культура.
Раздел 3
Сбор данных. Выбор источников
.**Раздел 4**
Качественные навыки специалистов по аналитике данных. Инструменты.
Раздел 5
Анализ данных. Типы анализы. Разработка показателей
Раздел 6
Оценка деятельности по управлению информационной безопасности. Способы оценки СУИБ организации. Метрики безопасности
Раздел 7
Процесс выработки программы получения метрик безопасности. Формулы расчета метрик безопасности. Примеры полученных результатов и принятых решений.
Раздел 8
Измерения информационной безопасности. Методы и подходы к проведению измерений. Критерии принятия решений. Действия, необходимые для разработки мер измерений и методов их получения.
Раздел 9
Обеспечение информационной безопасности банковских карт. Основные виды мошенничества с банковскими картами для эмитента. Мероприятия по противодействию мошенничеству.
Раздел 10
Основные виды мошенничества с банковскими картами для эквайера. Мероприятия по противодействию мошенничеству
Раздел 11
Исследование банковских карт. Основные сведения о пластиковых картах. Платежная система. Основы компьютерной криминалистики
Раздел 12
Расследование инцидентов информационной безопасности. Этапы расследования инцидента. Основные принципы изъятия компьютерной техники.
Раздел 13
Расследование инцидентов информационной безопасности. Судебная экспертиза. Заключение эксперта.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки специалистов 10.05.03 «Информационная безопасность автоматизированных систем».

4.2 Основная литература

- 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.
- 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

- 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
- 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

1. Электронный образовательный ресурс в разработке

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

6.1 Методические рекомендации для преподавателя по организации обучения

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01 «Информационная безопасность».**

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.

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
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

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 (модулю):

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: • Принципы функционирования средств обеспечения информационной безопасности; • Стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: . • Принципы функционирования средств обеспечения информационной безопасности; • Стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ;	Обучающийся демонстрирует неполное соответствие следующих знаний: • Принципы функционирования средств обеспечения информационной безопасности; • Стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные	Обучающийся демонстрирует частичное соответствие следующих знаний: • Принципы функционирования средств обеспечения информационной безопасности; • Стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; , но допускаются незначительные ошибки, неточности,	Обучающийся демонстрирует полное соответствие следующих знаний: • Принципы функционирования средств обеспечения информационной безопасности; • Стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; , свободно оперирует приобретенными знаниями.

		затруднения при оперировании знаниями при их переносе на новые ситуации.	затруднения при аналитических операциях.	
уметь: • Применять стандарты в области обеспечения информационной безопасности; • Разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); •Анализировать уязвимости информационных систем.	Обучающийся не умеет или в недостаточной степени умеет • Применять стандарты в области обеспечения информационной безопасности; • Разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); • Анализировать уязвимости информационных систем.	Обучающийся демонстрирует неполное соответствие следующих умений: • Применять стандарты в области обеспечения информационной безопасности; • Разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); • Анализировать уязвимости информационных систем. . Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: • Применять стандарты в области обеспечения информационной безопасности; • Разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); •Анализировать уязвимости информационных систем. . Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: • Применять стандарты в области обеспечения информационной безопасности; • Разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); •Анализировать уязвимости информационных систем. . Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: Навыками разработки модели угроз и нарушителя.	Обучающийся не владеет или в недостаточной степени владеет Навыками разработки модели угроз и нарушителя.	Обучающийся владеет Навыками разработки модели угроз и нарушителя., но допускаются значительные ошибки, проявляется недостаточность владения	Обучающийся частично владеет Навыками разработки модели угроз и нарушителя., навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет Навыками разработки модели угроз и нарушителя. , свободно применяет полученные навыки в ситуациях повышенной сложности.

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.

Фонды оценочных средств представлены в приложении к рабочей программе.

Структура и содержание дисциплины «Аналитика информационной безопасности»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	4 семестр														
1	Введение в информационно-аналитическую деятельность	4	1			2	2								
2	Технологический цикл ИАДКБ		2			2	2								
3	Первичная обработка информации		3			2	2								
4	Методика информационного поиска		4			2	2								
5	Основные принципы аналитической деятельности		5			2	2								
6	Планирование ИАДКБ. Этапы ИАДКБ. Системный подход в ИАДКБ		6			2	2								
7	Анализ информативности источников		7			2	2								
8	Оценка полноты, непротиворечивости и достоверности информации. Технология создания аналитических документов		8			2	2								
9	Отчетные документы ИАДКБ. Заключение		9			2	2								
10	Система информационно-		10			2	2								

	аналитического обеспечения в сфере безопасности														
11	Информационно-аналитические центры в РФ, их функции		11	2		2	2								
12	Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности		12	2		2	2								
13	Информационно-аналитическое обеспечение деятельности МВД в сфере компьютерных преступлений		13	2		2	2								
14	Анализ современного состояния «хакерства» в России и за рубежом		14	2		2	2								
15	Информационно-аналитическая работа в команде		15	2		2	4								
16	Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности		16	2		2	4								
17	Анализ современного состояния «хакерства» в России и за рубежом		17	2		2	4								
18	Информационно-аналитическая работа в команде		18	2		2	4								
	Форма аттестации	4	19-21							.					Д.з.
	Всего часов по дисциплине во четвертом семестре			36		36	36								
	Всего часов по дисциплине			36		36	36								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): «Безопасность открытых информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Аналитика информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Москва, 2022 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Аналитика информационной безопасности					
ФГОС ВО 10.05.03 «Информационная безопасность автоматизированных систем»					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценоч-ного средств**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	**знать:** ● принципы функционирования средств обеспечения информационной безопасности; ● стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; **уметь:** ● применять стандарты в области обеспечения информационной безопасности; ● разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); ● анализировать уязвимости информационных систем. **владеть:** ● навыками разработки модели угроз и нарушителя.	самостоятельная работа, лабораторные занятия, лекции	экзамен	Базовый уровень: знать: ● Стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ уметь: ● Анализировать уязвимости информационных систем Повышенный уровень: принципы функционирования средств обеспечения информационной безопасности; стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; принципы построения защищённых сетей. применять стандарты в области обеспечения информационной безопасности; разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); анализировать уязвимости информационных систем. навыками разработки модели угроз и нарушителя

Приложение 2
к рабочей программе

Оценочные средства для промежуточной аттестации

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.