МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
«28» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Аналитика информационной безопасности»

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная
Год приема - 2020

Москва 2020 г.

1. Цели освоения дисциплины.

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
-

2. Место дисциплины в структуре ООП.

Дисциплина «Аналитика информационной безопасности» относится к числу профессиональных учебных дисциплин базовой части цикла (Б.1) основной образовательной программы (Б.1.1.26).

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

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

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**	**Перечень планируемых результатов обучения по дисциплине**
ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**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.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лекции – 18 часов, лабораторные занятия – 36 час, самостоятельная работа - 54 часов, форма контроля – экзамен) в 4 семестре.

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

5. Образовательные технологии.

Методика преподавания дисциплины и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков у обучающихся:

- выполнение лабораторных работ в лабораториях вуза;
- индивидуальные и групповые консультации студентов преподавателем, в том числе в виде защиты выполненных заданий в рамках самостоятельной работы;
- посещение профильных конференций и работа на мастер-классах экспертов и специалистов индустрии;
- посещение лекций.

Самостоятельная внеаудиторная работа студентов составляет 50% от общего объема дисциплины и состоит из:

- посещение лекций;
- подготовки к выполнению и подготовки к защите лабораторных работ;
- чтения литературы и освоения дополнительного материала в рамках тематики дисциплины;
- подготовки к текущей аттестации;
- подготовки к промежуточной аттестации.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

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.

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

6.1.1. 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
ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

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.

6.1.2. 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):

ПК-10 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				
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 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, затруднения при	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.

		обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	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: экзамен.

Промежуточная аттестация обучающихся в форме экзамена 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.

7. Учебно-методическое и информационное обеспечение дисциплины.

1. 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.

2. 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.
- 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.

8. Материально-техническое обеспечение дисциплины

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.

Оборудование и аппаратура:

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

9. Методические рекомендации для самостоятельной работы студентов

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.

10. Методические рекомендации для преподавателя

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

Программу составил: ст. преп. Репин М.М.

Программа утверждена на заседании кафедры “Информационная безопасность” «29» августа 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение.

Структура и содержание дисциплины «Аналитика информационной безопасности»
по направлению подготовки
10.03.01 «Информационная безопасность» (бакалавр)

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	1		2	3								
2	Технологический цикл ИАДКБ		2	1		2	3								
3	Первичная обработка информации		3	1		2	3								
4	Методика информационного поиска		4	1		2	3								
5	Основные принципы аналитической деятельности		5	1		2	3								
6	Планирование ИАДКБ. Этапы ИАДКБ. Системный подход в ИАДКБ		6	1		2	3								
7	Анализ информативности источников		7	1		2	3								
8	Оценка полноты, непротиворечивости и достоверности информации. Технология создания аналитических документов		8	1		2	3								
9	Отчетные документы ИАДКБ. Заключение		9	1		2	3								

10	Система информационно-аналитического обеспечения в сфере безопасности		10	1		2	3								
11	Информационно-аналитические центры в РФ, их функции		11	1		2	3								
12	Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности		12	1		2	3								
13	Информационно-аналитическое обеспечение деятельности МВД в сфере компьютерных преступлений		13	1		2	3								
14	Анализ современного состояния «хакерства» в России и за рубежом		14	1		2	3								
15	Информационно-аналитическая работа в команде		15	1		2	3								
16	Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности		16	1		2	3								
17	Анализ современного состояния «хакерства» в России и за рубежом		17	1		2	3								
18	Информационно-аналитическая работа в команде		18	1		2	3								
	Форма аттестации	4	19-21							.				Э	
	Всего часов по дисциплине во четвертом семестре			18		36	54								
	Всего часов по дисциплине			36		18	54								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность компьютерных систем 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:

Составители: ст. преп. Репин М.М.

Москва, 2020 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Аналитика информационной безопасности					
ФГОС ВО **10.03.01 «Информационная безопасность»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**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.