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

УТВЕРЖДАЮ
Декан факультета
«Информационные технологии»
_____/Д.Г.Демидов/
«28» июня 2021

Рабочая программа дисциплины
«Аналитика информационной безопасности»

Направление подготовки
09.03.03 «Прикладная информатика»

Образовательная программа (профиль)
«Корпоративные информационные системы»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная
Год приема - 2021

Москва 2021 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 относится к числу учебных дисциплин части, формируемой участниками образовательных отношений.

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

Проектирование баз данных;

Разработка КИС;

Защита информации.

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
ОПК-3	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	**ОПК-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. **ОПК-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. **ОПК-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.
ПК-2	Способен осуществлять управление проектами в области ИТ на основе полученных планов проектов в условиях, когда проект не выходит за пределы утвержденных параметров	ИПК-2.1. Знать: программное обеспечение для управления проектами; методы и средства организации и управления ИС на всех стадиях жизненного цикла; требования информационной безопасности. ИПК-2.2. Уметь: выполнять работы на всех стадиях жизненного цикла проекта ИС, оценивать качество и затраты проекта. ИПК-2.3. Владеть: специализированным программным обеспечением для ведения проекта; работы с инструментальными средствами моделирования предметной области, прикладных и информационных процессов.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетные единицы, т.е. **144** академических часа (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, форма контроля – экзамен) на четвертом курсе в 7 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
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
ПК-2	Способен осуществлять управление проектами в области ИТ на основе полученных планов проектов в условиях, когда проект не выходит за пределы утвержденных параметров

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):

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				
ПК-2 Способен осуществлять управление проектами в области ИТ на основе полученных планов проектов в условиях, когда проект не выходит за пределы утвержденных параметров				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
ИПК-2.1. Знать: программное обеспечение для управления проектами; методы и средства	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний:	Обучающийся демонстрирует неполное соответствие следующих знаний: • Принципы функционирования	Обучающийся демонстрирует частичное соответствие следующих знаний: • Принципы	Обучающийся демонстрирует полное соответствие следующих знаний: • Принципы функционирования

организации и управления ИС на всех стадиях жизненного цикла; требования информационной безопасности.	. • Принципы функционирования средств обеспечения информационной безопасности; • Стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ;	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 затруднения при оперировании знаниями при их переносе на новые ситуации.	функционирования средств обеспечения информационной безопасности; • Стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; , но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	средств обеспечения информационной безопасности; • Стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; , свободно оперирует приобретенными знаниями.
ИПК-2.2. Уметь: выполнять работы на всех стадиях жизненного цикла проекта ИС, оценивать качество и затраты проекта.	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.

ИПК-2.3. Владеть: специализированным программным обеспечением для ведения проекта; работы с инструментальными средствами моделирования предметной области, прикладных и информационных процессов.	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 (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.

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

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.

3. При организации и проведения экзаменов в практико-ориентированной форме следует использовать утвержденные кафедрой Методические рекомендации.

Структура и содержание дисциплины « Аналитика информационной безопасности»
по направлению подготовки
09.03.03 «Прикладная информатика»
(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
	7 семестр														
1	Введение в информационно-аналитическую деятельность	7	1			4	4								
2	Технологический цикл ИАДКБ		2			4	4								
3	Первичная обработка информации		3			4	4								
4	Методика информационного поиска		4			4	4								
5	Основные принципы аналитической деятельности		5			4	4								
6	Планирование ИАДКБ. Этапы ИАДКБ. Системный подход в ИАДКБ		6			4	4								
7	Анализ информативности источников		7			4	4								
8	Оценка полноты, непротиворечивости и достоверности информации. Технология создания аналитических документов		8			4	4								
9	Отчетные документы ИАДКБ. Заключение		9			4	4								

10	Система информационно-аналитического обеспечения в сфере безопасности		10			4	4								
11	Информационно-аналитические центры в РФ, их функции		11			4	4								
12	Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности		12			4	4								
13	Информационно-аналитическое обеспечение деятельности МВД в сфере компьютерных преступлений		13			4	4								
14	Анализ современного состояния «хакерства» в России и за рубежом		14			4	4								
15	Информационно-аналитическая работа в команде		15			4	4								
16	Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности		16			4	4								
17	Анализ современного состояния «хакерства» в России и за рубежом		17			4	4								
18	Информационно-аналитическая работа в команде		18			4	4								
	Форма аттестации	7	19-21							.				Э	.
	Всего часов по дисциплине			36		72	72								

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: 09.03.03 «Прикладная информатика»

ОП (профиль): «Корпоративные информационные системы»

Форма обучения: очная

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

Кафедра: «Инфокогнитивные технологии»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Аналитика информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Москва, 2021 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Аналитика информационной безопасности					
ФГОС ВО **09.03.03 «Прикладная информатика»**					
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-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	**ОПК-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. **ОПК-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. **ОПК-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.	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

ПК-2	Способен осуществлять управление проектами в области ИТ на основе полученных планов проектов в условиях, когда проект не выходит за пределы утвержденных параметров	ИПК-2.1. Знать: программное обеспечение для управления проектами; методы и средства организации и управления ИС на всех стадиях жизненного цикла; требования информационной безопасности. ИПК-2.2. Уметь: выполнять работы на всех стадиях жизненного цикла проекта ИС, оценивать качество и затраты проекта. ИПК-2.3. Владеть: специализированным программным обеспечением для ведения проекта; работы с инструментальными средствами моделирования предметной области, прикладных и информационных процессов.	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.