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

«Инструментальный мониторинг защищённости систем»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)
«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация (степень) выпускника
Специалист по защите информации

Форма обучения

Очная
Год приема - 2020

Москва 2020 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Инструментальный мониторинг защищённости систем» следует отнести:

- формирование основных знаний и умений в области мониторинга информационной безопасности защищенных автоматизированных систем управления.

К **основным задачам** освоения дисциплины «Инструментальный мониторинг защищённости систем» следует отнести:

- знание основных понятий мониторинга событий; принципов работы систем мониторинга информационной безопасности; принципов работы систем управления автоматизированных систем и событиями в безопасности SIEM;
- умение применять средства мониторинга для оценки защищенности автоматизированных систем; использовать средства сбора и анализа информационной безопасности; формировать правила анализа событий защищенных мониторинга;
- владение методами мониторинга выявления угроз информационной безопасности автоматизированных систем.

2. Место дисциплины в структуре ООП.

Дисциплина «Инструментальный мониторинг защищённости систем» относится к числу профессиональных учебных базовой части цикла (Б.1) основной образовательной программы (Б.1.29).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Основы ИКТ», «Криптографические методы защиты 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-5.3	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	**знать:** • принципы и средства программного обеспечения защищенных автоматизированных систем • принципы построения, функционирования операционных систем, функционирования локальных и глобальных сетей, СУБД, web-приложений; **уметь:** • выявлять уязвимости защиты программных средств защищенных автоматизированных систем и находить пути их устранения; • проектировать и реализовывать защиту программных средств автоматизированных

		систем, исходя из поставленных целей защиты; **владеть:** • навыками анализа защищенности автоматизированных систем

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 5 семестре.

Структура и содержание дисциплины «Инструментальный мониторинг защищённости систем» по срокам и видам работы отражены в приложении.

5. Образовательные технологии.

Методика преподавания дисциплины «Инструментальный мониторинг защищённости систем» 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 обучающихся:

- подготовка к выполнению лабораторных работ;

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 20 % аудиторных занятий

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.

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-5.3	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах

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-5.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: • принципы и средства программного обеспечения защищенных автоматизированных систем • принципы построения, функционирования операционных систем, функционирования локальных и глобальных сетей, СУБД, web-приложений;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: . • принципы и средства программного обеспечения защищенных автоматизированных систем • принципы построения, функционирования операционных систем, функционирования локальных и глобальных сетей, СУБД, web-приложений;	Обучающийся демонстрирует неполное соответствие следующих знаний: • принципы и средства программного обеспечения защищенных автоматизированных систем • принципы построения, функционирования операционных систем, функционирования локальных и глобальных сетей, СУБД, web-приложений; 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: • принципы и средства программного обеспечения защищенных автоматизированных систем • принципы построения, функционирования операционных систем, функционирования локальных и глобальных сетей, СУБД, web-приложений; , но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: • принципы и средства программного обеспечения защищенных автоматизированных систем • принципы построения, функционирования операционных систем, функционирования локальных и глобальных сетей, СУБД, web-приложений; , свободно оперирует приобретенными знаниями.

уметь: • выявлять уязвимости защиты программных средств защищенных автоматизированных систем и находить пути их устранения; • проектировать и реализовывать защиту программных средств автоматизированных систем, исходя из поставленных целей защиты;	Обучающийся не умеет или в недостаточной степени умеет • выявлять уязвимости защиты программных средств защищенных автоматизированных систем и находить пути их устранения; • проектировать и реализовывать защиту программных средств автоматизированных систем, исходя из поставленных целей защиты;	Обучающийся демонстрирует неполное соответствие следующих умений: • выявлять уязвимости защиты программных средств защищенных автоматизированных систем и находить пути их устранения; • проектировать и реализовывать защиту программных средств автоматизированных систем, исходя из поставленных целей защиты; . Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: • выявлять уязвимости защиты программных средств защищенных автоматизированных систем и находить пути их устранения; • проектировать и реализовывать защиту программных средств автоматизированных систем, исходя из поставленных целей защиты; . Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений • выявлять уязвимости защиты программных средств защищенных автоматизированных систем и находить пути их устранения; • проектировать и реализовывать защиту программных средств автоматизированных систем, исходя из поставленных целей защиты; . Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: навыками анализа защищенности автоматизированных систем	Обучающийся не владеет или в недостаточной степени владеет • навыками анализа защищенности автоматизированных систем	Обучающийся владеет • навыками анализа защищенности автоматизированных систем , но допускаются значительные ошибки, проявляется недостаточность владения	Обучающийся частично владеет • навыками анализа защищенности автоматизированных систем , навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет навыками анализа защищенности автоматизированных систем , 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:**
   - Масленникова, Д.Л. Оценка уровня защищенности веб-ресурсов : выпускная квалификационная работа / Д.Л. Масленникова ; Сыктывкарский государственный университет имени Питирима Сорокина, Колледж экономики, права и информатики. – Сыктывкар : , 2018. – 46 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=490853 (дата обращения: 19.08.2019). – Текст : электронный.
   - Тишина, Н.А. Прикладные задачи безопасности информационно-телекоммуникационных систем : учебное пособие / Н.А. Тишина, Е. Чернопрудова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», Кафедра программного обеспечения вычислительной техники и автоматизированных систем. – Оренбург : ОГУ, 2017. – 122 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=485761 (дата обращения: 19.08.2019). – Библиогр.: с. 116-119. – ISBN 978-5-7410-1892-7. – Текст : электронный.
2. **Дополнительная литература:**

- 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: 19.08.2019). – Библиогр. в кн. – Текст : электронный.
- Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Национальный исследовательский университет – Высшая школа экономики. – Москва : Издательский дом Высшей школы экономики, 2015. – 574 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=440285 (дата обращения: 19.08.2019). – Библиогр. в кн. – ISBN 978-5-7598-0698-1. – 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. Офисные приложения, MicrosoftOffice.
2. Операционная система Windows.

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 б **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил: доц. Федоров Н.В.

Программа утверждена на заседании кафедры “Информационная

безопасность” «28» мая 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение.

Структура и содержание дисциплины «Инструментальный мониторинг защищённости систем»
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
	5 семестр														
1	Понятие защищенности автоматизированной системы. Нормативная база. Методика анализа защищенности	5	1-2			8	8								
2	Методы тестирования системы защиты. Классификация систем и средств анализа защищенности.		3-6			16	16								
3	Средства анализа параметров защиты. Классификация методов анализа параметров защиты (Security Benchmarks). Спецификации Security Benchmarks.		7-9			12	12								
4	Спецификации первого уровня для базового (минимального) уровня защиты. Спецификации второго уровня защиты для систем с		10-12			12	12								

	повышенными требованиями по безопасности														
5	Уязвимости уровня операционной системы. Методика поиска уязвимостей проектирования программного обеспечения: неустановленные обновления (patch'и и hotfix'ы) операционной системы, уязвимые сервисы и незащищенные конфигурации по умолчанию.		13-15			12	12								
6	Методика поиска уязвимостей, связанных с действиями администратора. Методика поиска уязвимостей, связанных с деятельностью пользователя.		16-18			12	12								
	Форма аттестации	5	19-21							.				Э	
	Всего часов по дисциплине во 5 семестре					72	72								
	Всего часов по дисциплине					72	72								

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: 10.05.03 «Информационная безопасность автоматизированных систем» ОП (профиль): «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная

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

.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Инструментальный мониторинг защищённости систем»

Состав: 1. Паспорт фонда оценочных средств
2. Описание оценочных средств:
Экзамен

Составители: доц. Федоров Н.В.

Москва, 2020 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Инструментальный мониторинг защищённости систем					
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 компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ОПК-5.3	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	**знать:** • принципы и средства программного обеспечения защищенных автоматизированных систем • принципы построения, функционирования операционных систем, функционирования локальных и глобальных сетей, СУБД, web-приложений; **уметь:** • выявлять уязвимости защиты программных средств защищенных автоматизированных систем и находить пути их устранения; • проектировать и реализовывать защиту программных средств автоматизированных систем, исходя из поставленных целей защиты; **владеть:** • навыками анализа защищенности автоматизированных систем	самостоятельная работа, лабораторные занятия	экзамен	**Базовый уровень:** **знать:** • принципы и средства программного обеспечения защищенных автоматизированных систем **уметь:** • выявлять уязвимости защиты программных средств защищенных автоматизированных систем и находить пути их устранения; **владеть:** • навыками анализа **Повышенный уровень:** • умеет проектировать и реализовывать защиту программных средств автоматизированных систем, исходя из поставленных целей защиты; • владеет навыками анализа защищенности автоматизированных систем

Приложение 2
к рабочей программе

Оценочные средства для текущей аттестации

Экзамен.

Список вопросов для экзамена по дисциплине

1. Понятие защищенности ИС.
2. Общая методика анализа защищенности.
3. Классификация методов тестирования системы защиты.
4. Классификация систем и средств анализа защищенности.
5. Классификация методов анализа параметров защиты (Security Benchmarks).
6. Спецификации Security Benchmarks.
7. Спецификации первого уровня для базового (минимального) уровня защиты.
8. Спецификации второго уровня защиты для систем с повышенными требованиями по безопасности.
9. Классификация средств анализа защищенности операционных систем и приложений.
10. Уязвимости уровня операционной системы.
11. Методика поиска уязвимостей проектирования программного обеспечения: неустановленные обновления (patch'и и hotfix'ы) операционной системы.
12. Методика поиска уязвимостей проектирования программного обеспечения: уязвимые сервисы и незащищенные конфигурации по умолчанию.
13. Методика поиска уязвимостей, связанных с действиями администратора: неправильно используемые настройки и функции системы.
14. Методика поиска уязвимостей, связанных с действиями администратора: не отвечающие политике безопасности требования.
15. Методика поиска уязвимостей, связанных с действиями администратора: несанкционированные изменения в конфигурации системы.
16. Методика поиска уязвимостей, связанных с деятельностью пользователя.