Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 30.10.2023 12:45:18
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

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

«Анализ защищённости систем»

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 «Анализ защищённости систем» следует отнести:

- овладение принципами организации процесса анализа защищенности автоматизированной системы.

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

- использования систем обнаружения вторжений.

2. Место дисциплины в структуре ООП.

Дисциплина «Анализ защищённости систем» относится к числу профессиональных учебных дисциплин базовой части цикла (Б1) основной образовательной программы (Б.1.1.30).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: Безопасность систем баз данных, Безопасность сетей электронных вычислительных машин, Безопасность операционных систем .

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-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	**знать:** • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений; **уметь:** • разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы; **владеть:** • навыками использования инструментальных средств анализа защищенности.
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования	**знать:** • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений; **уметь:** • разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы;

	соответствующих проектных решений	**владеть:** • навыками использования инструментальных средств анализа защищенности.
ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**знать:** • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений; **уметь:** • разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы; **владеть:** • навыками использования инструментальных средств анализа защищенности.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (Лекции – 36 час, лабораторные занятия – 36 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 5 семестре.

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

Содержание разделов дисциплины

Тема 1. Понятие защищенности ИС

Понятие защищенности автоматизированной системы. Нормативная база. Методика анализа защищенности. Исходные данные обследуемой ИС. Методы тестирования системы защиты. Классификация систем и средств анализа защищенности.

Средства анализа параметров защиты. Классификация методов анализа параметров защиты (Security Benchmarks). Спецификации Security Benchmarks. Спецификации первого уровня для базового (минимального) уровня защиты. Спецификации второго уровня защиты для систем с повышенными требованиями по безопасности.

Тема 2. Средства анализа защищенности сетевых сервисов

Уязвимости сетевых протоколов, служб, сервисов. Классификация средств анализа защищенности сетевых сервисов.

Сертифицированные средства анализа защищенности: XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС. Функции, методика использования.

Тема 3. Средства анализа защищенности web-приложений

Анализ и классификация уязвимостей web-приложений. Библиотека документов Open Web Application Security Project (OWASP), проект Web Application Security Consortium (WASC).

Комплексная оценка защищенности web-приложения. Принцип «черного ящика» Принцип «серого ящика». Принцип «белого ящика». Инструментальные средства анализа защищенности web-приложения.

5. Образовательные технологии.

Методика преподавания дисциплины «Анализ 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.

Образцы экзаменационных билетов, 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-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
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):

ОПК-7 Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
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 построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: . • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений.	Обучающийся демонстрирует неполное соответствие следующих знаний: • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений 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 построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений , свободно оперирует приобретенными знаниями.

уметь: •разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы.	Обучающийся не умеет или в недостаточной степени умеет •разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы.	Обучающийся демонстрирует неполное соответствие следующих умений: •разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: •разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: •разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: • навыками использования инструментальных средств анализа защищенности.	Обучающийся не владеет или в недостаточной степени владеет • навыками использования инструментальных средств анализа защищенности.	Обучающийся владеет •навыками использования инструментальных средств анализа защищенности, но допускаются значительные ошибки, проявляется недостаточность владения	Обучающийся частично владеет навыками использования инструментальных средств анализа защищенности , навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет навыками использования инструментальных средств анализа защищенности , 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 средствпредставлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная литература:

1 Золотарев В.В., Федорова Н.А. Анализ защищенности автоматизированных систем.- Красноярск, СибГАУ, 2007 – 93 с.

2 Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2005. — 256 с.

б) дополнительная литература:

1 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2007. 960 с.

в) программное обеспечение и интернет-ресурсы:

XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС

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.

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: к.т.н., доцент Н.В. Федоров

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 «Анализ защищённости систем»
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
	6 семестр														
1	Понятие защищенности автоматизированной системы. Нормативная база. Методика анализа защищенности.	5	1	4			12								
2	Средства анализа параметров защиты. Классификация методов анализа параметров защиты (Security Benchmarks).		2-3	6		2	12								
3	Уязвимости сетевых протоколов, служб, сервисов. Классификация средств анализа защищенности сетевых сервисов.		4-5	6		2	12								
4	Сертифицированные средства анализа защищенности: XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС. Функции, методика использования.		6-10	8		12	12								

5	Анализ и классификация уязвимостей web-приложений. Библиотека документов Open Web Application Security Project (OWASP), проект Web Application Security Consortium (WASC).		11-14	6		10	12								
6	Комплексная оценка защищенности web-приложения. Принцип «черного ящика» Принцип «серого ящика». Принцип «белого ящика». Инструментальные средства анализа защищенности web-приложения.		15-18	6		10	12								
	Форма аттестации	5	19-21							.				Э	
	Всего часов по дисциплине во шестом семестре			36		36	72								
	Всего часов по дисциплине			36		36	72								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗРВАНИЯ

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

(кибербезопасность новой информационной среды)»

Форма обучения: очная

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

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Анализ 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

Анализ защищённости систем					
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**				

ОПК-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	**знать:** • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений; **уметь:** • разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы; **владеть:** • навыками использования инструментальных средств анализа защищенности.	самостоятельная работа, лабораторные занятия	экзамен	Базовый знать: • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений; уметь: • проводить анализ защищенности компонентов автоматизированной системы; владеть: • навыками использования инструментальных средств анализа защищенности. уровень: Повышенный уровень: уметь: • разрабатывать методику поиска и обнаружения уязвимостей;

ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	**знать:** • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений; **уметь:** • разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы; **владеть:** • навыками использования инструментальных средств анализа защищенности.	самостоятельная работа, лабораторные занятия	экзамен	Базовый знать: • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений; уметь: • проводить анализ защищенности компонентов автоматизированной системы; владеть: • навыками использования инструментальных средств анализа защищенности. уровень: Повышенный уровень: уметь: • разрабатывать методику поиска и обнаружения уязвимостей;

ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**знать:** • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений; **уметь:** • разрабатывать методику поиска и обнаружения уязвимостей; • проводить анализ защищенности компонентов автоматизированной системы; **владеть:** • навыками использования инструментальных средств анализа защищенности.	самостоятельная работа, лабораторные занятия	экзамен	Базовый знать: • принципы построения, функционирования и примеры реализации систем анализа защищенности и обнаружения вторжений; уметь: • проводить анализ защищенности компонентов автоматизированной системы; владеть: • навыками использования инструментальных средств анализа защищенности. уровень: Повышенный уровень: уметь: • разрабатывать методику поиска и обнаружения уязвимостей;

Приложение 2
к рабочей программе

Оценочные средства для промежуточной 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 сетевых сервисов
10. Уязвимости сетевых протоколов, служб, сервисов.
11. Классификация средств анализа защищенности сетевых сервисов.
12. Сертифицированные средства анализа защищенности: XSpider. Функции, методика использования.
13. Сертифицированные средства анализа защищенности: MaxPatrol. Функции, методика использования.
14. Сертифицированные средства анализа защищенности: Ревизор Сети. Функции, методика использования.
15. Сертифицированные средства анализа защищенности: СканерВС. Функции, методика использования.
16. Классификация средств анализа защищенности web-приложений
17. Анализ и классификация уязвимостей web-приложений.
18. Библиотека документов Open Web Application Security Project (OWASP), проект Web Application Security Consortium (WASC).
19. Комплексная оценка защищенности web-приложения.
20. Принцип «черного ящика».
21. Принцип «серого ящика».
22. Принцип «белого ящика».
23. Инструментальные средства анализа защищенности web-приложения

Пример билета.

1. Классификация систем и средств анализа защищенности.
2. Сертифицированные средства анализа защищенности: MaxPatrol. Функции, методика использования.