

**Министерство науки и высшего образования РФ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Национальный исследовательский университет «МЭИ»**

**Направление подготовки/специальность: 10.03.01 Информационная безопасность**

**Наименование образовательной программы: Безопасность автоматизированных систем**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очная**

**Оценочные материалы  
по дисциплине  
Программно-аппаратные средства защиты информации**

**Москва  
2022**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Дратвяк А.В.
	Идентификатор	R1a0ecc29-DratviakAV-b9b11303

(подпись)

А.В. Дратвяк

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка  
подписи)

Заведующий  
выпускающей кафедры

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю.

Невский

(расшифровка  
подписи)

## ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ОПК-4.3 способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем

ИД-1 Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах

ИД-2 Применяет программные средства обеспечения безопасности данных

2. ОПК-4.4 способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем

ИД-1 Выполняет обнаружение и идентификацию инцидентов в процессе эксплуатации автоматизированной системы

ИД-2 Оценивает защищенность автоматизированных систем с помощью типовых программных средств

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Письменная работа

1. Контрольное мероприятие № 1 (Контрольная работа)
2. Контрольное мероприятие № 2 (Контрольная работа)
3. Контрольное мероприятие № 3 (Контрольная работа)
4. Контрольное мероприятие № 4 (Контрольная работа)
5. Контрольное мероприятие № 5 (Контрольная работа)
6. Контрольное мероприятие № 6 (Контрольная работа)
7. Контрольное мероприятие № 7 (Контрольная работа)
8. Контрольное мероприятие № 8 (Контрольная работа)

## БРС дисциплины

5 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ- 1	КМ- 2	КМ- 3	КМ- 4
	Срок КМ:	4	8	12	15
Введение					
Концептуальные основы информационной безопасности		+	+		
Основные понятия программно-аппаратной защиты информации		+	+		

Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений				
Механизмы обеспечения конфиденциальности доступа к информации на уровне операционных систем			+	+
Механизмы обеспечения конфиденциальности доступа к информации на уровне приложений			+	+
Программно-аппаратные средства криптографической защиты информации			+	+
Обеспечение конфиденциальности информации в IP-сетях			+	+
Обеспечение целостности информации с помощью программных и аппаратных средств				
Терминология резервирования. Оперативное и автономное резервирование. Типы резервирования. Виды RAID-массивов. Исходные типы RAID-массивов. RAID-контроллеры. Основы резервирования данных. Варианты резервирования данных			+	+
Обеспечение целостности при передаче информации по сетям			+	+
Комплексные системы защиты информации				
Обеспечение антивирусной защиты информационных систем			+	+
Предотвращение утечек информации (DLP) и учет рабочего времени			+	+
Системы обнаружения и предотвращения вторжений			+	+
Вес КМ:	25	25	25	25

6 семестр

Раздел дисциплины	Весы контрольных мероприятий, %				
	Индекс КМ:	КМ-5	КМ-6	КМ-7	КМ-8
	Срок КМ:	4	8	12	15
Обеспечение доступности информации применением средств программно-аппаратной защиты					
Обеспечение доступности информации средствами операционной системы Управление правами доступа к ресурсам в операционных системах семейства MS Windows. Учетные записи пользователей и групп. Управление доступом и глобальными параметрами. Основные сведения об учетных записях групп. Оснастка "Локальные пользователи и группы"	+	+	+	+	+
Обработка информации на рабочих станциях и обеспечение ее доступности	+	+	+	+	+
Обеспечение доступности информации в локальных сетях		+	+	+	+
Основы веб-безопасности					
Цели атаки на веб-ресурсы предприятия			+	+	+
Методы и инструменты злоумышленника для атаки на веб-ресурсы			+	+	+

Классификация сетевых атак.		+	+	+
Вес КМ:	25	25	25	25

\$Общая часть/Для промежуточной аттестации\$

## СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

### *I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций*

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ОПК-4.3	ИД-1 <sub>ОПК-4.3</sub> Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах	Знать: Типовые программные и программно-аппаратные средства резервирования и восстановления информации в автоматизированных системах Уметь: Проводить установку и настройку программных и программно-аппаратных средства резервирования и восстановления информации в автоматизированных системах	Контрольное мероприятие № 1 (Контрольная работа) Контрольное мероприятие № 2 (Контрольная работа) Контрольное мероприятие № 3 (Контрольная работа) Контрольное мероприятие № 4 (Контрольная работа)
ОПК-4.3	ИД-2 <sub>ОПК-4.3</sub> Применяет программные средства обеспечения безопасности данных	Знать: Особенности проведения работ по установке, настройке, администрированию, обслуживанию и проверке работоспособности программно-аппаратных и	Контрольное мероприятие № 3 (Контрольная работа) Контрольное мероприятие № 4 (Контрольная работа) Контрольное мероприятие № 6 (Контрольная работа) Контрольное мероприятие № 7 (Контрольная работа) Контрольное мероприятие № 8 (Контрольная работа)

		<p>технических средств защиты информации в автоматизированных системах</p> <p>Уметь:</p> <p>Применять типовые программно-аппаратные средства защиты информации в автоматизированных системах и базах данных</p>	
ОПК-4.4	<p>ИД-1<sub>ОПК-4.4</sub> Выполняет обнаружение и идентификацию инцидентов в процессе эксплуатации автоматизированной системы</p>	<p>Знать:</p> <p>Способы осуществления диагностики и мониторинга систем защиты автоматизированных систем</p> <p>Уметь:</p> <p>Администрировать системы обнаружения и идентификации инцидентов информационной безопасности в процессе эксплуатации автоматизированной системы</p>	<p>Контрольное мероприятие № 5 (Контрольная работа)</p> <p>Контрольное мероприятие № 6 (Контрольная работа)</p> <p>Контрольное мероприятие № 7 (Контрольная работа)</p> <p>Контрольное мероприятие № 8 (Контрольная работа)</p>
ОПК-4.4	<p>ИД-2<sub>ОПК-4.4</sub> Оценивает защищенность автоматизированных систем с помощью типовых программных</p>	<p>Знать:</p> <p>Способы обнаружения и идентификации инцидентов информационной</p>	<p>Контрольное мероприятие № 1 (Контрольная работа)</p> <p>Контрольное мероприятие № 2 (Контрольная работа)</p> <p>Контрольное мероприятие № 5 (Контрольная работа)</p>

	средств	безопасности в процессе эксплуатации автоматизированной системы Уметь: Выполнять оценку защищенности информации, идентификацию и ликвидацию инцидентов информационной безопасности в процессе эксплуатации автоматизированных систем	
--	---------	--	--



## II. Содержание оценочных средств. Шкала и критерии оценивания

5 семестр

### КМ-1. Контрольное мероприятие № 1

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

#### Краткое содержание задания:

Дайте письменный ответ на 6 вопросов.

Один из двух вариантов контрольного мероприятия выбирается по критерию:

нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

#### Контрольные вопросы/задания:

Знать: Типовые программные и программно-аппаратные средства резервирования и восстановления информации в автоматизированных системах	1.Контрольное мероприятие № 1 по дисциплине Программно-аппаратные средства защиты информации		
	№ п/п	1 Вариант	2 Вариант
	1	Основные понятия и определения в сфере информационной безопасности. Угрозы информации. Методы защиты информации	Программно-аппаратная защита информации. Основные понятия
	2	Что относится к основным аппаратным средствам защиты информации?	Что относится к основным программным средствам защиты информации?
	3	Каковы основные преимущества применения программных средств защиты информации?	Каковы основные недостатки применения программных средств защиты информации?
	4	Механизмы управления доступом и аутентификации ОС Windows. Уязвимости доступа к ОС MS Windows	Организация хранения паролей в ОС Microsoft Windows. База SAM, ее характеристика.
5	Шифрующая файловая система (EFS). Технология шифрования.	Организация хранения паролей в ОС Microsoft Windows, Linux и MacOS.	
Уметь: Выполнять оценку	1.		

защищенности информации, идентификацию и ликвидацию инцидентов информационной безопасности в процессе эксплуатации автоматизированных систем	6	Провести анализ уязвимостей ОС Windows 10 за 2021 год по базе данных CVE	Провести анализ уязвимостей ОС Ubuntu за 2021 год по базе данных CVE

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто, выбрано верное направление для решения задач*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено*

**КМ-2. Контрольное мероприятие № 2**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

**Краткое содержание задания:**

Дайте письменный ответ на 6 вопросов.

Один из двух вариантов контрольного мероприятия выбирается по критерию:

нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

**Контрольные вопросы/задания:**

Знать: Типовые программные и программно-аппаратные средства резервирования и восстановления информации в автоматизированных системах	1.Контрольное мероприятие № 1 по дисциплине Программно-аппаратные средства защиты информации		
	№ п/п	1 Вариант	2 Вариант
	1	Назначение и принципы работы ПАК "Аккорд-NT" и "Аккорд-АМДЗ".	Устройства криптографической защиты данных. Краткая характеристика ПСКЗИ "Шипка".
2	Устройства ввода идентификационных признаков, классификация, краткая характеристика	Биометрический доступ. Обзор биометрических технологий	

	3	Полностью контролируемые компьютерные системы. Аттестация КС. Программная и аппаратная реализация функций КС.	Обеспечение безопасности хранения данных в ОС Microsoft Windows. Технология теневого копирования данных	
	4	Суть и назначение протокола TCP/IP и UDP/IP в контексте защиты конфиденциальной информации	Применение протоколов семейства TCP/IP в сфере информационной безопасности АС	
	5	В соответствии с требованиями ФСТЭК России определить требования по защите АС рекламного отдела компании ООО "Рога и Копыта", обрабатывающей персональные данные граждан РФ, в целях рассылки информации о скидочных акциях и днях распродаж. В АС попеременно могут работать следующие сотрудники: руководитель рекламного отдела, сотрудник рекламного отдела, а также в АС имеют доступ системный администратор и сотрудник службы безопасности.	В соответствии с требованиями ФСТЭК России определить требования по защите АС режимно-секретного подразделения компании ООО "Ромашка", обрабатывающей секретные данные третьей категории, в целях формирования отчетной документации по результатам аудита ИБ и проведения аттестационных испытаний. В АС попеременно могут работать следующие сотрудники: все сотрудники (около 3 человек) аттестационного отдела, сотрудник отдела аудита ИБ, руководитель аттестационного отдела, начальник режимно-секретного подразделения и системный администратор.	
Уметь: Выполнять оценку защищенности информации, идентификацию и ликвидацию инцидентов информационной безопасности в процессе эксплуатации автоматизированных систем	1.	5	<p>Продемонстрировать настройку системы защиты от НСД с использованием возможностей ПАК "Аккорд-NT", а именно:</p> <ul style="list-style-type: none"> <li>• блокировку съемных носителей</li> </ul>	<p>Продемонстрировать настройку ПСКЗИ "Шипка", а именно:</p> <ul style="list-style-type: none"> <li>• шифрование созданного студентом на рабочем столе файла MS Word;</li> </ul>

		информации; • блокировку CD/DVD-дисков.	• электронную подпись созданного студентом на рабочем столе файла MS Word.
--	--	--	--

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

**КМ-3. Контрольное мероприятие № 3**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

**Краткое содержание задания:**

Дайте письменный ответ на 6 вопросов.

Один из двух вариантов контрольного мероприятия выбирается по критерию:

нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

**Контрольные вопросы/задания:**

Знать: Особенности проведения работ по установке, настройке, администрированию, обслуживанию и проверке работоспособности программно-аппаратных и технических средств защиты информации в автоматизированных системах	1.Контрольное мероприятие № 1 по дисциплине Программно-аппаратные средства защиты информации		
	№ п/п	1 Вариант	2 Вариант
	1	Каким образом работают VPN сети по протоколу Point to Point Tunneling Protocol (PPTP)?	Каким образом работают VPN сети по протоколу Layer 2 Tunneling Protocol (L2TP)?
	2	Для каких целей и каким образом применяются протоколы SSL И TLS?	Для каких целей и каким образом применяются протокол IPsec?
	3	Перечислите базовые разрешения,	Опишите функциональные

		применимые к файлам и папкам на томах с файловой системы NTFS	возможности и цель применения Microsoft Management Console (MMC)
	4	Для решения каких задач может применяться оснастка "Локальные пользователи и группы"?	Для решения каких задач может применяться оснастка "Групповые политики"?
	5	Каким образом может быть произведена отмена действия групповых политик на локальном компьютере в Windows?	Перечислите приемы для обхода групповых политик в Windows
Уметь: Проводить установку и настройку программных и программно-аппаратных средства резервирования и восстановления информации в автоматизированных системах	1.		
	6	Продемонстрировать настройку VPN-канала с использованием встроенных в ОС Windows программных решений	Продемонстрировать настройку VPN-канала с использованием технологии OpenVPN

#### Описание шкалы оценивания:

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено*

#### КМ-4. Контрольное мероприятие № 4

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС: 25**

**Процедура проведения контрольного мероприятия:** Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

#### Краткое содержание задания:

Дайте письменный ответ на 6 вопросов.

Один из двух вариантов контрольного мероприятия выбирается по критерию:

нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

#### Контрольные вопросы/задания:

Знать: Особенности проведения работ по установке, настройке, администрированию, обслуживанию и проверке работоспособности программно-аппаратных и технических средств защиты информации в автоматизированных системах	1. Контрольное мероприятие № 1 по дисциплине Программно-аппаратные средства защиты информации		
	№ п/п	1 Вариант	2 Вариант
	1	Понятие и типы резервирования данных. Определение RAID, основные типы RAID-массивов и их характеристики.	Системы анализа защищенности. Принципы работы систем анализа защищенности. Примеры реализации.
	2	Виртуальные частные сети (VPN). Протоколы, используемые в VPN, их основные характеристики. Примеры реализации.	Механизмы блокировки рабочей станции на аппаратном уровне. Доверенная загрузка. Этапы доверенной загрузки.
	3	Межсетевые экраны. Типы межсетевых экранов. Разработка правил для межсетевого экрана.	Межсетевые экраны. Критерии выбора межсетевых экранов. Основные требования регуляторов к межсетевым экранам.
	4	Основы управления электропитанием рабочих станций и серверов. Критерии выбора ИБП.	Защита информации при передаче по вычислительным сетям. Защищенные протоколы передачи данных.
Уметь: Проводить установку и настройку программных и программно-аппаратных средства резервирования и восстановления информации в автоматизированных системах	5	Технология беспроводной передачи данных, ее защита	Контроль целостности информации. Основные методы. Примеры реализации.
	1.	6	На стенде кафедры продемонстрировать реализацию рейд массива данных по типу RAID-5 для предложенного преподавателем жёсткого диска

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

6 семестр

### КМ-5. Контрольное мероприятие № 5

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

**Краткое содержание задания:**

Дайте письменный ответ на 5 вопросов.

Один из двух вариантов контрольного мероприятия выбирается по критерию:

нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

**Контрольные вопросы/задания:**

Знать: Способы обнаружения и идентификации инцидентов информационной безопасности в процессе эксплуатации автоматизированной системы	1.		
	№ п/п	1 Вариант	2 Вариант
	1	Ранжировать методы и инструменты злоумышленника, направленные на сетевую инфраструктуру предприятия	Дать определение ARP spoofing'a. Указать инструменты, используемые для реализации атак типа ARP spoofing. Предложить механизмы защиты
	2	Сформировать рекомендации по применению сканеров безопасности информации специалистами red и blue команд. Указать известные Вам сканеры безопасности по трём направлениям работы: сеть, АС, веб.	Предложить классификацию троянских программ по категории вида представляемой угрозы
	3	Охарактеризуйте основные способы проникновения вредоносных программ на корпоративные АС предприятия	Дайте характеристику вариантам противодействия и нарушения работы антивирусных программных продуктов
4	В соответствии с уровнями модели OSI дайте характеристику вариантам реализуемых на них атаках	Дайте определение туннелирования, как вида атаки на АС предприятия. Укажите варианты защиты от	

			туннелирования
Уметь: Администрировать системы обнаружения и идентификации инцидентов информационной безопасности в процессе эксплуатации автоматизированной системы	1.		
	5	Указать какими данными злоумышленник может завладеть в сети на каждом её уровне в соответствии с моделью OSI при успешном использовании сниффера	Привести признаки наличия сниффера в сети. Привести примеры открытого ПО для защиты сети от снифферов

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено*

**КМ-6. Контрольное мероприятие № 6**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

**Краткое содержание задания:**

Дайте письменный ответ на 5 вопросов.

Один из двух вариантов контрольного мероприятия выбирается по критерию:

нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

**Контрольные вопросы/задания:**

Знать: Способы осуществления диагностики и мониторинга систем защиты автоматизированных систем	1.		
	<b>№ п/п</b>	<b>1 Вариант</b>	<b>2 Вариант</b>
	1	Категорирование DDoS-атак по сетевым протоколам	Категорирование DDoS-атак по схемам осуществления
	2	Классификация атак на прикладном уровне модели OSI. Принципы организации SQL-инъекций и XSS	Классификация атак на протоколы TCP и UDP в коммерческих и промышленных сетях
3	Модель угроз и основные типы атак на беспроводные сети	Модель нарушителя безопасности беспроводных сетей	



		стандарта 802.11. Примеры ПО для реализации защиты.	стандарта 802.11. Примеры ПО для реализации атаки.
	4	Принципы работы и назначение DLP-систем в составе SOC. Примеры программных решений.	Функциональные возможности DLP-систем для защиты конфиденциальной информации в корпоративных сетях. Примеры программных решений.
Уметь: Применять типовые программно-аппаратные средства защиты информации в автоматизированных системах и базах данных	1.		
	5	Сформировать перечень применяемых техник атаки на АС с использованием социальной инженерии	Предложить рекомендации по применению программно-аппаратных средств защиты от атак с использованием социальной инженерии

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено*

**КМ-7. Контрольное мероприятие № 7**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

**Краткое содержание задания:**

Дайте письменный ответ на 5 вопросов.

Один из двух вариантов контрольного мероприятия выбирается по критерию:

нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

**Контрольные вопросы/задания:**

Знать: Способы осуществления диагностики и мониторинга систем защиты	1.		
	№ п/п	1 Вариант	2 Вариант
	1	Какие пути внедрения	Из каких источников

автоматизированных систем		вредоносного ПО в АС Вам известны? Какие способы борьбы с антивирусным ПО Вам известны?	информации специалисты по обеспечению безопасности узнают о видах уязвимостей для веб-приложений?
	2	Дайте характеристику сетевым атакам на <b>канальном уровне</b> модели OSI	Дайте характеристику сетевым атакам на <b>физическом уровне</b> модели OSI
	3	Дайте характеристику сетевым атакам на <b>сетевом уровне</b> модели OSI	Дайте характеристику сетевым атакам на <b>транспортном уровне</b> модели OSI
	4	Перечислите несколько наиболее опасных уязвимостей веб-приложений в соответствии с OWASP TOP-10	Охарактеризуйте изменения в базе данных OWASP TOP-10 за последние 5 лет с точки зрения появления новых видов угроз веб-приложениям
Уметь: Применять типовые программно-аппаратные средства защиты информации в автоматизированных системах и базах данных	1.5. В соответствии с известными Вам типами атак на сетевую инфраструктуру предприятия (по уровням модели OSI) сформировать типовую таблицу модели угроз на основе приложения 11 к "Методике оценки угроз безопасности информации" ФСТЭК России от 5 февраля 2021 г. В результате выполнения задания у Вас должна получиться таблица или структурированный список: Тактика - Техника (вид атаки) - Программная реализация (атакующее ПО)		

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто, выбрано верное направление для решения задач*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено*

**КМ-8. Контрольное мероприятие № 8**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС: 25**

**Процедура проведения контрольного мероприятия:** Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

**Краткое содержание задания:**

Дайте письменный ответ на 5 вопросов.

Один из двух вариантов контрольного мероприятия выбирается по критерию: нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

**Контрольные вопросы/задания:**

Знать: Способы осуществления диагностики и мониторинга систем защиты автоматизированных систем	1.	
	<b>№ п/п</b>	<b>1 Вариант</b>
	1	Приведите классификацию атак по критерию местоположения атакующего и ОИ
	2	В чём заключается опасность IP-spoofing?
	3	В чём суть атаки на МЭ методом туннелирования?
	4	Какова суть атаки крошечными фрагментами?
Уметь: Применять типовые программно-аппаратные средства защиты информации в автоматизированных системах и базах данных	<p>1.5. Практическое задание может выполнять в группах по 2-3 человека. Необходимо сформировать отчёт в формате презентации PowerPoint или PDF по нижеследующим подзадачам:</p> <ol style="list-style-type: none"> <li>1. Дать характеристику корпоративным решениям защиты от DDoS-атак и их отличиям от средств защиты персональных АС</li> <li>2. Описать назначение и функциональные возможности программных решений защиты от DDoS-атак</li> <li>3. Сформировать классификацию типов аппаратного оборудования, используемого в борьбе с DDoS-атаками</li> </ol>	

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено*

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета

<b>НИУ МЭИ</b>	<b>ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1</b> Кафедра <i>Безопасности и информационных технологий</i> Дисциплина «Программно-аппаратные средства защиты информации»	<i>Утверждаю: Зав. каф. БИТ А.Ю.Невский Протокол кафедры №3 «18»декабря 2019г.</i>
1. Ранжировать типовые методы и инструменты злоумышленника, направленные на сетевую инфраструктуру предприятия 2. Сформировать рекомендации по применению сканеров безопасности информации специалистами red и blue команд. Указать известные Вам сканеры безопасности по трём направлениям работы: сеть, АС, веб. 3. Продемонстрируйте перехват трафика локальной сети стенда кафедры с использованием программы WireShark		

## Процедура проведения

Устный зачет с практической письменной частью на листах установленного администрацией образца

### ***1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины***

**1. Компетенция/Индикатор:** ИД-1<sub>ОПК-4.3</sub> Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах

#### **Вопросы, задания**

1. Охарактеризуйте основные способы проникновения вредоносных программ на корпоративные АС предприятия
2. Дайте характеристику вариантам противодействия и нарушения работы антивирусных программных продуктов

#### **Материалы для проверки остаточных знаний**

1. Каковы особенности функционирования системы предотвращения утечек информации в режиме мониторинга (DLP-системы), работающей в корпоративной сети предприятия?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к четырнадцатой лекции по дисциплине «Программно-аппаратные средства защиты информации»

Верный ответ: DLP-системы отслеживают: - исходящий и входящий web-трафик; - коммуникации сотрудников по различным каналам связи, в социальных сетях, на форумах и иных ресурсах; - информацию, хранящуюся на рабочих станциях, серверах, в облачных хранилищах; - факты загрузки файлов на съемные носители; - внесение изменений в документы, отправку их на печать и прочие события; - рабочее время и действия сотрудников: использование программного обеспечения,

интернет-сервисов, попытки изменения конфигурации ПО, оборудования и так далее.

## 2. Чем TCP SYN Flood отличается от Reflection SYN flooding?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к тринадцатой лекции по дисциплине «Программно-аппаратные средства защиты информации»

Верный ответ: На сервера в сети посылаются SYN-пакеты с исходным IP-адресом атакующей машины. Сервер или маршрутизатор получает эти поддельные SYN-пакеты и посылает SYN/ACK ответы на атакуемый хост. Компьютер, отправляющий SYN/ACK пакет, ожидает на него ACK-ответ, а при его отсутствии посылает ещё несколько SYN/ACK пакетов. SYN/ACK пакеты продолжают атаковать целевой сервер даже после того, как злоумышленник прекратил нападение.

## 3. Какие атаки специально сконструированными пакетами Вам известны?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к тринадцатой лекции по дисциплине «Программно-аппаратные средства защиты информации»

Верный ответ: Ping of death. Посылка на атакуемый узел фрагментированной датаграммы, размер которой после сборки превышает максимальный разрешенный размер датаграммы Land. Посылка на атакуемый узел SYN-сегмента TCP, у которого IP-адрес и порт отправителя совпадают с получателем Teardrop. Присылается несколько фрагментов одного пакета. При сборке пакета второй фрагмент накладывается на первый, и его данные записываются поверх предыдущего фрагмента

## 2. Компетенция/Индикатор: ИД-2ОПК-4.3 Применяет программные средства обеспечения безопасности данных

### Вопросы, задания

1. В соответствии с уровнями модели OSI дайте характеристику вариантам реализуемых на них атаках
2. Дайте определение туннелирования, как вида атаки на АС предприятия. Укажите варианты защиты от туннелирования

### Материалы для проверки остаточных знаний

1. Какие типы DDoS-атак в соответствии с уровнями модели OSI Вам известны?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к седьмой лекции по дисциплине «Программно-аппаратные средства защиты информации»

Верный ответ: Низкоуровневые атаки: - Атаки на сетевом уровне OSI представляют из себя «забивание» канала. Примером может быть СМР-флуд — атака, которая использует ICMP-сообщения, которые снижают пропускную способность атакующей сети и перегружают брандмауэр. Хост постоянно «пингуется» нарушителями, вынуждая его отвечать на ping-запросы. Когда их приходит значительное количество, пропускной способности сети не хватает и ответы на запросы приходят со значительной задержкой. Для предотвращения таких DDoS-атак можно отключить обработку ICMP-запросов посредством Firewall или ограничить их количество, пропускаемое на сервер. - Атаки транспортного уровня выглядят как нарушение функционирования и перехват трафика. Например, SYN-флуд или Smurf-атака (атака ICMP-запросами с изменёнными адресами). Последствия такой DDoS-атаки — превышение количества доступных подключений и перебои в работе сетевого оборудования. Высокоуровневые атаки: - На сеансовом уровне атакуются сетевое оборудование. Используя уязвимости программного

обеспечения Telnet-сервера на свитче, злоумышленники могут заблокировать возможность управления свитчем для администратора. Чтоб избежать подобных видов атак, рекомендуется поддерживать прошивки оборудования в актуальном состоянии. - Высокоуровневые атаки прикладного уровня ориентированы на стирание памяти или информации с диска, «воровство» ресурсов у сервера, извлечение и использование данных из БД. Это может привести к тотальной нехватке ресурсов для выполнения простейших операций на оборудовании. Наиболее эффективный способ предупреждения атак – своевременный мониторинг состояния системы и программного обеспечения.

2.Перечислите основные типы SQL-инъекций, используемых для атаки на корпоративные сети предприятий

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к одиннадцатой лекции по дисциплине «Программно-аппаратные средства защиты информации»

Верный ответ: Существует 5 основных типов SQL инъекций: - Классическая (In-Band или Union-based). Самая опасная и редко встречающаяся сегодня атака.

Позволяет сразу получать любые данные из базы. - Error-based. Позволяет получать информацию о базе, таблицах и данных на основе выводимого текста ошибки СУБД. - Boolean-based. Вместо получения всех данных, атакующий может поштучно их перебирать, ориентируясь на простой ответ типа true/false. - Time-based. Похожа на предыдущую атаку принципом перебора, манипулируя временем отклика базы. - Out-of-Band. Очень редкие и специфические типы атак, основанные на индивидуальных особенностях баз данных.

3.Предложите рекомендации по защите типового коммерческого веб-сайта от SQL-инъекций

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к одиннадцатой лекции по дисциплине «Программно-аппаратные средства защиты информации»

Верный ответ: Для защиты сайта от SQL-инъекции рекомендуется: - Используйте белые списки - Не использовать метод GET в формах идентификации - Обработайте переменные - Проверять источник получения данных - Использовать PDO

**3. Компетенция/Индикатор:** ИД-1<sub>ОПК-4.4</sub> Выполняет обнаружение и идентификацию инцидентов в процессе эксплуатации автоматизированной системы

### Вопросы, задания

- 1.Дать определение ARP spoofing'a. Указать инструменты, используемые для реализации атак типа ARP spoofing. Предложить механизмы защиты
- 2.Предложить классификацию троянских программ по категории вида представляемой угрозы
- 3.Какие три категории DDoS-атак Вам известны? Каковы механизмы защиты от них?

## II. Описание шкалы оценивания

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания:* Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания:* Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

*Оценка:* 3

*Нижний порог выполнения задания в процентах:* 50

*Описание характеристики выполнения знания:* Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

### **III. Правила выставления итоговой оценки по курсу**

**6 семестр**

**Форма промежуточной аттестации:** Экзамен

**Пример билета**

<b>НИУ МЭИ</b>	<b>ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1</b> Кафедра <i>Безопасности и информационных технологий</i> Дисциплина «Программно-аппаратные средства защиты информации»	<i>Утверждаю: Зав. каф. БИТ А.Ю.Невский Протокол кафедры №3 «18»декабря 2019г.</i>
1. Основные понятия и определения в сфере информационной безопасности. Угрозы информации. Методы защиты информации. 2. Биометрический доступ. Обзор биометрических технологий. 3. Создать резервную копию папки Мои Документы с использованием утилиты NTBackup.		

### **Процедура проведения**

Устный экзамен с практической частью на стендах кафедры

#### ***I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины***

**1. Компетенция/Индикатор:** ИД-1<sub>ОПК-4.3</sub> Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах

#### **Вопросы, задания**

- 1.Резервирование данных. Типы резервирования. RAID, определение. Основные типы RAID- массивов и их характеристики.
- 2.Обеспечение безопасности хранения данных в ОС Microsoft Windows. Технология теневого копирования данных.
- 3.Программно-аппаратные средства контроля доступа. Устройства ввода идентификационных признаков, классификация, краткая характеристика.

#### **Материалы для проверки остаточных знаний**

- 1.Какова цель применения DLP-систем в сфере информационной безопасности хозяйствующего субъекта?

Ответы:



Для верного ответа на вопрос рекомендуется использовать материалы лекции по дисциплине “Программно-аппаратные средства защиты информации”

Верный ответ: Основной задачей DLP-систем, что очевидно, является предотвращение передачи конфиденциальной информации за пределы информационной системы. Такая передача (утечка) может быть намеренной или ненамеренной. Наиболее часто DLP-системы применяются для решения следующих неосновных для себя задач: - контроль использования рабочего времени и рабочих ресурсов сотрудниками; - мониторинг общения сотрудников с целью выявления внутренней борьбы, которая может навредить организации; - контроль правомерности действий сотрудников (предотвращение печати поддельных документов и пр.); - выявление сотрудников, рассылающих резюме, для оперативного поиска специалистов на освободившуюся должность.

**2. Компетенция/Индикатор:** ИД-2<sub>ОПК-4.3</sub> Применяет программные средства обеспечения безопасности данных

### Вопросы, задания

1. Архивация данных. Стратегии архивации.
2. Системы анализа защищенности. Принципы работы систем анализа защищенности.

**3. Компетенция/Индикатор:** ИД-1<sub>ОПК-4.4</sub> Выполняет обнаружение и идентификацию инцидентов в процессе эксплуатации автоматизированной системы

### Материалы для проверки остаточных знаний

1. Какие компоненты входят в состав SIEM-систем, применяемых в коммерческих корпоративных сетях?

Ответы:

Для верного ответа на вопрос рекомендуется использовать материалы лекции по дисциплине “Программно-аппаратные средства защиты информации”

Верный ответ: Компоненты SIEM: - агенты, устанавливаемые на инспектируемую информационную систему (актуально для операционных систем (агент представляет собой резидентную программу (сервис, демон), которая локально собирает журналы событий и по возможности передает их на сервер) - коллекторы на агентах, которые, по сути, представляют собой модули (библиотеки) для понимания конкретного журнала событий или системы - серверы-коллекторы, предназначенные для предварительной аккумуляции событий от множества источников - сервер-коррелятор, отвечающий за сбор информации от коллекторов и агентов и обработку по правилам и алгоритмам корреляции - сервер баз данных и хранилища, отвечающий за хранение журналов событий

2. Какие рекомендации экспертов из сферы информационной безопасности по защите от DDoS Вам известны?

Ответы:

Для верного ответа на вопрос рекомендуется использовать материалы лекции по дисциплине “Программно-аппаратные средства защиты информации”

Верный ответ: 1) сконфигурировать анти-спуфинг на маршрутизаторах и МЭ для блокировки исходящего трафика, если адрес источника не является внутренним адресом сети; 2) сконфигурировать анти-DoS на маршрутизаторах и МЭ для ограничения числа полуоткрытых каналов и невозможности перегрузки системы; 3) ограничить объем некритического трафика в ЛВС, например ICMP; 4) применять IDS для анализа трафика и выявления аномалий в нем; 5) применять резервные полосы пропускания или резервные сетевых устройств в пиковый рост нагрузки.

3. Каким дополнительными угрозам в сравнение с проводными подвержены беспроводные линии передачи данных?

Ответы:

Для верного ответа на вопрос рекомендуется использовать материалы лекции по дисциплине “Программно-аппаратные средства защиты информации”

Верный ответ: Нарушение физической целостности сети случайными или преднамеренными помехами. Подслушивание трафика на физическом уровне приёмниками в широком спектре сигнала. НСВторжение в сеть по занесённым в таблицу разрешённых MAC-адресам.

**4. Компетенция/Индикатор:** ИД-2<sub>ОПК-4.4</sub> Оценивает защищенность автоматизированных систем с помощью типовых программных средств

#### Вопросы, задания

- 1.Выполнить автоматическую постановку ресурсов на контроль АМДЗ «Аккорд» с помощью мастера
- 2.Межсетевые экраны. Типы межсетевых экранов. Разработка правил для межсетевого экрана.
- 3.Виртуальные частные сети (VPN). Протоколы, используемые в VPN, их основные характеристики.

#### Материалы для проверки остаточных знаний

1.Какие аппаратные устройства ввода идентификационных признаков в автоматизированную систему Вам известны?

Ответы:

Для правильного ответа на вопрос необходимо корректно определить возможные аппаратные идентификаторы, применяемые в системах защиты информации

Верный ответ: По способу считывания идентификационных признаков выделяют: • с ручным вводом; • контактные; • дистанционные (бесконтактные); • комбинированные. Ручной ввод идентификационных признаков производится с помощью нажатия клавиш, поворотом переключателей или других подобных элементов. Контактное считывание идентификационных признаков подразумевает непосредственный контакт идентификатора и считывателя. Чтение информации происходит путём проведения идентификатора через считыватель или их простым прикосновением.

2.Каковы основные функции IDS-систем?

Ответы:

В ответе на вопрос необходимо раскрыть основные функции IDS-систем, применяемых в сфере информационной безопасности

Верный ответ: К основным функциям систем IDS относятся: - выявление вторжений и сетевых атак; - запись всех событий; - поиск уязвимостей; - прогнозирование атак; - распознавание источника атаки: инсайд или взлом; - информирование служб ИБ об инциденте в реальном времени; - формирование отчетов.

3.Раскройте суть и назначение криптографических средств защиты информации

Ответы:

Для корректного ответа на вопрос необходимо обратиться к определению термина “криптографическая защита”, предлагаемого ФСБ России, как основного регулятора этой сферы информационной безопасности

Верный ответ: Средства криптографической защиты информации (СКЗИ) – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

## ***II. Описание шкалы оценивания***

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня*

## ***III. Правила выставления итоговой оценки по курсу***

Для оценки используется только результаты промежуточной аттестации и экзамена