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

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Оценочные материалы
по дисциплине
Информационно-аналитические системы безопасности

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(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. ПК-5 способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества

2. ПК-6 способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок

и включает:

для текущего контроля успеваемости:

Форма реализации: Выполнение задания

1. Выполнение/защита реферата (Реферат)
2. Контрольное задание № 1. Практическая разработка этапов проведения аудита информационной безопасности информационной системы организации (Отчет)
3. Контрольное задание № 2. Практика применения сканера безопасности (Отчет)
4. Контрольное задание № 4. Практика применения MaxPatrol SIEM. (Отчет)

Форма реализации: Компьютерное задание

1. Контрольно задание № 3. Практика применения DLP-системы SearchInform «Контур безопасности» (Отчет)

БРС дисциплины

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %					
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-4
	Срок КМ:	4	8	12	15	15
Информационно-аналитическая деятельность в системе обеспечения безопасности хозяйствующего субъекта.						
Вводная тема.		+				
Тема 1. Аналитическая работа в повседневной деятельности предприятия в области ИБ.		+				
Тема 2. Системы обеспечения информационной безопасности предприятия		+				

Тема 3. Информационно аналитические системы защиты и безопасности	+				
Информационные технологии в системе информационно-аналитического обеспечения безопасности					
Тема 4. Технологии системы информационно-аналитического обеспечения безопасности	+	+	+	+	+
Тема 5. DLP-системы функционирование и модель.		+	+	+	+
Тема 6. Основы функционирования DLP-системы Контур информационной безопасности SearchInform в информационной системе организации.		+	+	+	+
Тема 7. SIEM-системы архитектура и основы функционирования.		+	+	+	+
Тема 8. «СёрчИнформ SIEM» архитектура и основы функционирования		+	+	+	+
Тема 9. «MaxPatrol SIEM» архитектура и основы функционирования.		+	+	+	+
Вес КМ:	25	25	25	15	10

$Общая часть/Для промежуточной аттестации$

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
ПК-5	ПК-5(Компетенция)	Знать: современные технические средства и информационные технологии, используемые для решения задач информационно-аналитической деятельности специалиста в области информационной безопасности	Контрольное задание № 1. Практическая разработка этапов проведения аудита информационной безопасности информационной системы организации (Отчет)
ПК-6	ПК-6(Компетенция)	Уметь: осуществлять сбор, анализ и обработку данных, необходимых для решения профессиональных задач аудита информационной безопасности информационных систем и объектов информатизации	Контрольное задание № 2. Практика применения сканера безопасности (Отчет) Контрольно задание № 3. Практика применения DLP-системы SearchInform «Контур безопасности» (Отчет) Контрольное задание № 4. Практика применения MaxPatrol SIEM. (Отчет) Выполнение/защита реферата (Реферат)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольное задание № 1. Практическая разработка этапов проведения аудита информационной безопасности информационной системы организации

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического занятия.

Краткое содержание задания:
Используя материалы лекции по теме 2 и интернет - ресурсы провести анализ одного из ниже перечисленных вопросов:
1. Характеристика особенностей выполнения мероприятий постановки задачи и уточнение границ работ;
2. Характеристика особенностей выполнения мероприятий по сбору и анализу информации;
3. Характеристика особенностей выполнения мероприятий анализа данных аудита;
4. Характеристика особенностей выполнения мероприятий по разработке рекомендаций по совершенствованию системы защиты информации;
5. Характеристика особенностей выполнения мероприятий подготовки аудиторского отчета.

Контрольные вопросы/задания:

Знать: современные технические средства и информационные технологии, используемые для решения задач информационно-аналитической деятельности специалиста в области информационной безопасности	1.Понятие информационно-аналитической работы 2.Направления аналитической работы 3. Этапы аналитической работы 4.Методы аналитической работы

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 задание № 2. Практика применения сканера безопасности

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического занятия.

Краткое содержание задания:
Используя материалы лекции по теме 4 и интернет - ресурсы провести анализ одного из сканеров безопасности, поддерживаемых различными профильными организациями и вендорами.

Контрольные вопросы/задания:

Уметь: осуществлять сбор, анализ и обработку данных, необходимых для решения профессиональных задач аудита информационной безопасности информационных систем и объектов информатизации	1.Порядок оценки защищенности информационной системы с использованием на основе использования сканеров безопасности

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. Контрольно задание № 3. Практика применения DLP-системы SearchInform «Контур безопасности»

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического занятия.

Краткое содержание задания:
освоить основные приемы:
1. использования программного комплекса SearchInform для перехвата и поиска утечек конфиденциальной информации

2. приемы реализации периодического и оперативного контроля экранов пользователей, а также методы формирования критериев поиска конфиденциальной информации «по атрибутам» и «нераспознанных».
3. приемы формирования поисковых запросов конфиденциальной информации на основе критериев подобия текста.
4. приемы формирования поисковых запросов конфиденциальной информации на основе подобия текстовых фрагментов.
5. принципы формирования регулярных выражений для поиска конфиденциальной информации и овладеть методикой настройки системы перехвата программного комплекса SearchInform.

Контрольные вопросы/задания:

Уметь: осуществлять сбор, анализ и обработку данных, необходимых для решения профессиональных задач аудита информационной безопасности информационных систем и объектов информатизации	1.1. Как установить пароль для пользователя «Администратор» Windows Server? 2. Как изменить параметры учетной записи в Windows Server? 3. Как установить пароль на консоль Search Server? 4. Как установить пароль на консоль DataCenter? 5. Как установить пароль на консоль EndpointSniffer? 6. Как установить пароль на консоль NetworkSniffer? 7. Как установить пароль на консоль ReportCenter? 8. Как установить пароль на службу AlertCenter? 9. Что такое индекс? 10. Как разграничить права доступа к индексам? 2.1. Как используется «белый список»? 2. Как используется «черный список»? 3. Чем отличается глобальный фильтр от фильтра по протоколам? 4. Зачем подключать AlertCenter к индексам? 5. Какой должен быть интервал обновления индексов? 6. Почему нужно отключать выполнение расписания политики? 7. Что такое активный индекс? 8. Что такое доступный индекс? 3.1. К каким действиям можно привязать включение снятия скриншотов? 2. Как изменить частоту кадров для режима видеозаписи? 3. Какое назначение опции LiveView агента MonitorSniffer? 4. Можно ли с помощью программного комплекса SearchInform произвести поиск данных переданных по протоколу http, базируясь на IP-адресе получателя? 5. Можно ли с помощью программного комплекса SearchInform отсортировать данные переданные на flash-носитель от данных переданных на компакт диск?

	6. Можно ли с помощью программного комплекса SearchInform произвести поиск данных переданных с помощью чата Skype? 7. Можно ли с помощью программного комплекса SearchInform произвести поиск данных переданных по протоколу ftp, базируясь на направлении передачи? 8. Можно ли с помощью программного комплекса SearchInform произвести поиск данных переданных по протоколу http, базируясь на направлении передачи? 9. Можно ли с помощью программного комплекса SearchInform произвести поиск данных переданных по электронной почте с использованием скрытых копий? 4.1. Как снять цифровой отпечаток из текста в графическом файле? 2. Можно ли снять цифровой отпечаток из pdf-файла? 3. Можно ли снять цифровой отпечаток из java-файла? 4. Какие документы нецелесообразно искать с помощью критерия «По цифровым отпечаткам»? 5. Как объединяются простые запросы в сложные? 6. Как проверить синтаксис сложного запроса? 5.1. В чем разница между функциональностью кнопок «Добавить ссылку» и «Добавить значение» окна «Библиотека регулярных выражений»? 2. Почему в окне «Выбор регулярного выражения» могут присутствовать несколько одинаковых названий регулярных выражений? 6.1. Как в шаблоне определить пробел? 2. Как в шаблоне определить отдельное слово? 3. Как в шаблоне определить нечувствительность к регистру? 4. Как в шаблоне определить альтернативу? 5. Как в шаблоне определить группировку?

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. Выполнение/защита реферата

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Реферат
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Самостоятельное выполнение реферата.

Краткое содержание задания:
Используя материалы лекции по теме 4 и 5 и интернет - ресурсы провести разработку реферата по анализу практического применения, основных характеристик и функциональных возможностей, преимуществ и недостатков одной из SIEM-систем.

Контрольные вопросы/задания:

Уметь: осуществлять сбор, анализ и обработку данных, необходимых для решения профессиональных задач аудита информационной безопасности информационных систем и объектов информатизации	1.Архитектура SIEM-системы 2.Алгоритм работы SIEM-системы 3.Характеристика применения основных модулей типового решения SIEM-системы

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 задание № 4. Практика применения MaxPatrol SIEM.

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического занятия.

Краткое содержание задания:
Цель контрольного задания: получение теоретических и практических навыков работы с SIEM проверка знаний по работе с SIEM-системы Камрад.

Контрольные вопросы/задания:

Уметь: осуществлять сбор, анализ и обработку данных,	1.Какие существуют альтернативы использованию SIEM?

необходимых для решения профессиональных задач аудита информационной безопасности информационных систем и объектов информатизации	2.Каким образом в SIEM КОМРАД выполняется задача Поиск по событиям в режиме реального времен?

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

1 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ «МЭИ»	**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1** Кафедра *Безопасности и информационных технологий* Дисциплина: *Информационно-аналитические системы безопасности*	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* *Протокол заседания кафедры №3* *«16» декабря 2020г.*
1. Общая характеристика мероприятий информационно-аналитической деятельности сотрудников информационной безопасности организации 2. Характеристика ключевых возможностей системы комплексного мониторинга информационной безопасности MaxPatrol по защищенности и соответствия стандартам 3. Запустить виртуальный компьютер с установленным программным комплексом КИБ SearchInform. Практически сформировать параметры собственной политики безопасности, которые должны включать в себя: расписание проверки и список индексов/баз данных для проверки конфиденциальной информации в ИС		

Процедура проведения

Устный опрос

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

1. Компетенция/Индикатор: ПК-5(Компетенция)

Вопросы, задания

1.Понятие аудита информационной безопасности, свидетельства и критерия аудита информационной безопасности организаци
2.Характеристика задач внешнего и внутреннего аудита информационной безопасности
3.Состав и общая характеристика этапа постановки задачи и уточнения границ работ проведения аудита информационной безопасности информационной системы (организации)
4.Состав и общая характеристика этапа сбора и анализа информации аудита информационной безопасности информационной системы (организации)
5.Состав и общая характеристика этапа анализа данных аудита информационной безопасности информационной системы (организации)
6.Состав и общая характеристика этапа разработки рекомендаций аудита информационной безопасности информационной системы (организации)
7.Состав и общая характеристика этапа подготовки аудиторского отчета аудита информационной безопасности информационной системы (организации)
8.Принципы формирования регулярных выражений для поиска конфиденциальной информации. Методика настройки системы перехвата программного комплекса SearchInform

Материалы для проверки остаточных знаний

1.Механизм контроля соответствия стандартам (Compliance) в MaxPatrol 8

Верный ответ: Режим контроля соответствия стандартам позволяет проверять выполнение требований российских регулирующих органов, международных и отраслевых стандартов, корпоративных регламентов.

2.Функции анализа каких объектов информационной системы реализованы в системе MaxPatrol

Верный ответ: •операционные системы •сетевое оборудование •системы управления базами данных •настольные приложения •серверное ПО •системы безопасности •бизнес-приложения •АСУ ТП •системы криптографической защиты информации

3.Какие основные задачи решаются системой MaxPatrol

Верный ответ: 1. Оценка эффективности существующих процессов ИБ с помощью метрик безопасности. 2. Оценка защищенности. 3. Инвентаризация 4. Контроль политик безопасности. 5. Контроль измерений

4.Что предполагает оценка защищенности в системе MaxPatrol

Верный ответ: •Проактивная защита корпоративных ресурсов с помощью автоматического мониторинга информационной безопасности. •Автоматизация процессов контроля соответствия отраслевым и международным стандартам. •Оценка эффективности подразделений ИТ и ИБ с помощью расширяемого набора метрик безопасности и KPI. •Снижение затрат на аудит и контроль защищенности, подготовку ИТ и ИБ проектов. •Автоматизация процессов инвентаризации ресурсов, управления уязвимостями, контроля соответствия политикам безопасности и контроля изменений. •Комплексный анализ сложных систем, включая сетевое оборудование Cisco, платформ Windows, Linux, Unix, СУБД Microsoft SQL, Oracle, сетевые приложения и Web-службы собственной разработки. •Встроенная поддержка основных стандартов, таких как ГОСТ ИСО/МЭК 27001, SOX, PCI DSS, NSA, NIST, CIS. •Максимальная автоматизация процессов снижает трудозатраты и позволяет оперативно контролировать состояние защищенности систем. •Поддержка базы знаний командой профессиональных консультантов, признанных экспертов отрасли.

5.DLP-система это ….?

Верный ответ: DLP-система (Data Loss Prevention) – это программный продукт, созданный для предотвращения утечек конфиденциальной информации за пределы корпоративной сети

6.Какие способы обнаружения утечки данных реализуют DLP системы

Верный ответ: DLP системы различают по способу обнаружения утечки данных: •при использовании (Data-in Use) — на рабочем месте пользователя; •при передаче (Data-in Motion) — в сети компании; •при хранении (Data-at Rest) — на серверах и рабочих станциях компании.

7.Какие пять способов анализа используется в DLP системах

Верный ответ: Поиск по словарям (по точному совпадению слов, в некоторых случаях с учетом морфологии); Регулярные выражения. Регулярные выражения — система синтаксического разбора текстовых фрагментов по формализованному шаблону, основанная на системе записи образцов для поиска. Например, номера кредитных карт, телефонов, адреса e-mail, номера паспортов, лицензионные ключи и т.п. Сравнение по типам файлов. Политиками безопасности может быть запрещена отправка вовне некоторых типов файлов. При этом если пользователь изменит расширение файла, то система все равно должна «опознать» тип файла и предпринять необходимые действия. Статистический («поведенческий») анализ информации по пользователям. Если пользователь имеет доступ к конфиденциальной информации, и в то же время он посещает определенные сайты (web-storage, web-mail, хакерские и т.п.), то он попадает в «группу риска» и к нему возможно применение дополнительных ограничивающих политик безопасности. Технологии цифровых отпечатков.

8.Архитектура типовой DLP системы?

Верный ответ: 1. Центральный сервер управления, выполняющий следующие функции: – объединение всех остальных компонентов решения в единую систему; – определение данных, содержащих конфиденциальную информацию; – создание, редактирование и распространение политик работы с конфиденциальными данными; – сбор, хранение и обработку инцидентов, создание и рассылку отчетов; – предоставление ролевого доступа к управлению системой сотрудникам службы информационной безопасности; 2. Модули мониторинга и блокировки конфиденциальной информации, передаваемой по сетевым каналам. Они могут быть представлены как одним устройством, реализующим обе функции, так и отдельными (например, Network Monitor, Network Prevent for Web, Network Prevent for E-mail). 3. Агенты для рабочих станций и серверов, обеспечивающие контроль: – перемещения конфиденциальных данных на сменные носители информации (USB, CD/DVD и др.); – помещения данных в буфер обмена (функция «Вставка/Копирование»); – функции снятия снимка с экрана («Print Screen»); – контроль функции поиска конфиденциальных данных на локальных дисках.

9.Назначение Контура информационной безопасности SearchInform»

Верный ответ: Контур информационной безопасности SearchInform» – это комплексная DLP-система для защиты от действий инсайдеров и утечек конфиденциальных данных. «Контур информационной безопасности SearchInform» предназначен для контроля информационных потоков в рамках локальной вычислительной сети. Контроль возможен двумя способами, в зависимости от используемого серверного компонента: SearchInform EndpointSniffer или SearchInform NetworkSniffer.

10.Состав и назначение модулей контроля информации Контура информационной безопасности SearchInform»

Верный ответ: Модули контроля информации: SearchInform EndpointSniffer — платформа для перехвата и блокировки информационных потоков посредством агентов, установленных на рабочие станции. Агенты SearchInform EndpointSniffer производят теневое копирование перехваченной информации и направляют полученные данные серверу SearchInform EndpointSniffer SearchInform NetworkSniffer — платформа перехвата и блокировки информационных потоков на уровне сети.

11.Состав и назначение модулей анализа информации Контура информационной безопасности SearchInform»

Верный ответ: Модули анализа информации: Search Server — сервер индексации и поиска. SearchInform AlertCenter — является «мозговым центром» системы «Контур информационной безопасности SearchInform».

12.Состав и назначение модулей перехвата информации Контура информационной безопасности SearchInform»

Верный ответ: Модули перехвата: SearchInform KeyLogger — позволяет перехватывать данные, вводимые пользователем с клавиатуры. SearchInform FileSniffer — предназначен для контроля операций с файлами, хранящимися на серверах и в общих сетевых папках. SearchInform Cloud & SharePoint — предназначен для контроля трафика из облачных хранилищ. SearchInform FTPSniffer — предназначен для контроля входящего и исходящего FTP-трафика на уровне рабочих станций. SearchInform ProgramSniffer — предназначен для ведения учета активности пользователей в запускаемых ими приложениях и на посещаемых веб-ресурсах на протяжении рабочего дня. SearchInform PrintSniffer — предназначен для контроля содержимого документов, отправленных пользователем на печать посредством как сетевых, так и локальных принтеров. SearchInform HTTPSniffer — предназначен для перехвата сообщений, передаваемых по HTTP-протоколу,

индексирования перехваченных сообщений и полнотекстового поиска по ним. Модуль также позволяет контролировать работу сотрудников и отслеживать их общение в рабочее время. SearchInform MonitorSniffer — предназначен для перехвата информации, отображаемой на мониторах пользователей. Решение поставляется совместно с программным модулем KeyLogger. SearchInform MicrophoneSniffer — предназначен для записи разговоров, ведущихся сотрудниками внутри офиса и в командировках. SearchInform MailSniffer — предназначен для перехвата почтового трафика на уровне рабочих станций и сетевых протоколов, индексирования полученных сообщений и осуществления поиска по ним. SearchInform IMSniffer — предназначен для перехвата сообщений популярных IM-клиентов. SearchInform SkypeSniffer — приложение перехватывает сеансы голосовой и текстовой связи, SMS-сообщения и файлы, передаваемые при помощи Skype. SearchInform DeviceSniffer — программный модуль, перехватывающий информацию, передаваемую пользователем на внешние устройства, а также отслеживающий сам факт подключения такого рода устройств. SearchInform ADSniffer — контроль и анализ событий журналов Active Directory позволяет выявлять подозрительные действия, которые могут совершаться системным администратором компании. Телефония — модуль обеспечивает перехват аудиозвонков и текстовых сообщений телефонии SIP через стандарты GSM, A-Law, u-Law и G.722. Модуль шифрования данных — обеспечивает шифрование всех типов данных, записываемых на внешние устройства хранения USB.

13.Контроль каких информационных потоков выполняет Контур информационной безопасности SearchInform»

Верный ответ: «Контур информационной безопасности SearchInform» поддерживает перехват следующих данных: сообщения электронной почты, отправленные или полученные по протоколам SMTP, POP3, IMAP, MAPI, NNTP, HTTP(S); мгновенные сообщения, переданные по протоколам OSCAR (службы ICQ, AIM), MMP (Mail.ru Agent), MSNP (Windows Live/MSN), XMPP (Google Hangouts, Jabber), а также текстовые/голосовые сообщения и файлы, передаваемые посредством Microsoft Lync и Viber Desktop; сообщения и файлы, отправленные при помощи браузера в чаты, форумы, блоги, социальные сети (Facebook, LinkedIn, В Контакте, Мой Мир@Mail.Ru, Одноклассники.ru, Google+, Mamba.ru и др.); входящие и исходящие данные облачных сервисов при работе через веб-интерфейс (Google Docs, OneDrive (Microsoft), Office 365 (Office Online), DropBox, Evernote, Яндекс.Диск Cloud.mail.ru, SharePoint); остановка трафика на уровне сети на уровне ICAP — HTTP, FTP; данные, передаваемые на внешние устройства; история операций с файлами, расположенными на ноутбуках; файлы, отправленные или полученные по FTP-соединению; содержимое мониторов ноутбуков пользователей, а также нажатия клавиш; разговоры сотрудника, находящегося вне офиса; документы, отправленные на печать. текстовые и голосовые сеансы связи по Skype, файлы и SMS-сообщения, переданные или полученные при помощи Skype; активность пользователей и запускаемых ими приложений. контроль устройств на рабочих станциях.

14.Какие предустановленные универсальные политики безопасности включает «Контур информационной безопасности SearchInform» :

Верный ответ: контроль откатов и взяточничества; выявление негативных настроений и сговоров в коллективе; определение групп риска (проблемы с алкоголем, наркотиками, крупные долги и т. д.); контроль персональных данных (паспорта, номера банковских карт и др.); выявление общения с конкурентами, с уволенными сотрудниками; посещение запрещенных сайтов; антитеррористические политики и др.

15. Какие основные функций выполняет SIEM-система

Верный ответ: 1. Определение и фиксация данных о событиях ИБ на источниках событий. 2. Сбор, фильтрация и передача на сервер данных о событиях ИБ. 3. Получение, агрегация, нормализация и хранение поступающих данных. 4. Корреляция нормализованных данных о событиях ИБ. 5. Выявление событий предшествующих возникновению инцидентов ИБ. 6. Определение инцидентов ИБ, выявление и реагирование на них. 7. Обновление базы знаний с включением правил противодействия атакам по выявленным инцидентам ИБ. 8. Организация мониторинга доступности узлов и служб. 9. Генерация отчетов различных типов на основе хранимых на сервере данных.

16.Какие SIEM-система имеет уровни построения

Верный ответ: 1. Сбор данных: осуществляется от источников различных типов, например, файловых серверов, межсетевых экранов, антивирусных программ и др. 2. Управление данными: данные, хранящиеся в репозитории, выдаются по запросам моделей анализа данных. 3. Анализ данных: результатом являются отчеты в предопределенной и произвольной форме, оперативная корреляция данных о событиях, а также выдаваемые предупреждения.

2. Компетенция/Индикатор: ПК-6(Компетенция)

Вопросы, задания

1.Основные задачи решаемые системой MaxPatrol
2.Характеристика основных возможностей MaxPatrol
3.Характеристика архитектуры MaxPatrol
4.Основные сценарии внедрения системы комплексного мониторинга информационной безопасности
5.Эволюционное развитие и повышение эффективности MaxPatrol
6.Порядок оценки защищенности информационной системы с использованием MaxPatrol
7.Механизмы оценки защищенности информационных систем инструментами MaxPatrol
8.Порядок оценки защищенности информационной системы с использования DLP систем
9.Порядок оценки защищенности информационной системы с использованием функции MaxPatrol «Анализ Web-приложений»
10.Порядок оценки защищенности информационной системы с использованием MaxPatrol «Тестирование на проникновение»
11.Порядок оценки защищенности информационной системы с использованием MaxPatrol «Аудит SQL Server».
12.Порядок оценки защищенности информационной системы с использованием MaxPatrol «Аудит Solaris»
13.Порядок настройки профиля для оценки защищенности информационной системы с использованием MaxPatrol
14.Порядок описания уязвимостей при оценке защищенности информационной системы с использованием MaxPatrol
15.Контроль соответствия (механизмы Compliance Cisco) MaxPatrol
16.Классификация DLP-систем по способу обнаружения утечки информации
17.Методы анализа используемые в DLP-системах
18.Характеристика архитектуры DLP-систем
19.Характеристика технологий предотвращения утечки информации при использовании DLP-систем
20.Назначение, решаемые задачи, основные возможности, преимущества и недостатки и характеристика применения основных модулей типового решения DLP-системы КИБ SearchInform

21.Основные приемы использования программного комплекса КИБ SearchInform для перехвата и поиска утечек конфиденциальной информации
22.Основные приемы реализации периодического и оперативного контроля экранов пользователей, а также методы формирования критериев поиска конфиденциальной информации «по атрибутам» и «нераспознанных»
23.Основные приемы формирования поисковых запросов конфиденциальной информации на основе критериев подобия текста
24.Основные приемы формирования поисковых запросов конфиденциальной информации на основе подобия текстовых фрагментов
25.Назначение, цели и задачи системы, основные возможности «SearchInform SIEM»
26.Архитектура и алгоритм работы системы «SearchInform SIEM»
27.Преимущества и недостатки продукта «SearchInform SIEM».
28.Характеристика применения основных модулей типового решения SIEM-системы SearchInform

Материалы для проверки остаточных знаний

1.Информационно-аналитическая деятельность службы безопасности это
Ответы:
-
Верный ответ: Информационно-аналитическая деятельность службы безопасности фирмы представляет собой системное получение, анализ и накопление информации с элементами прогнозирования по вопросам, относящимся к безопасности фирмы, и на этой основе консультирование и подготовка рекомендаций руководству о правомерной защите от противоправных посягательств

2.Функции ИАС
Верный ответ: • обеспечить своевременное поступление надежной и всесторонней информации по интересующим вопросам; • описать сценарии действий конкурентов, которые могут затрагивать текущие интересы фирмы; • осуществлять постоянный мониторинг событий во внешней конкурентной среде и на рынке, которые могут иметь значение для интересов фирмы; • обеспечить безопасность собственных информационных ресурсов; • обеспечить эффективность и исключить дублирование при сборе, анализе и распространении информации.

3.Перечислите основные направления аналитической работы
Верный ответ: К основным направлениям аналитической работы, разрабатываемым на многих фирмах, можно отнести: анализ объекта защиты, анализ угроз, анализ каналов несанкционированного доступа к информации, анализ комплексной безопасности фирмы, анализ нарушений режима конфиденциальности, анализ подозрений утраты конфиденциальной информации

4.Виды направлений аналитической работы
Верный ответ: Направления аналитической работы, ведущейся ИАС фирмы, могут быть постоянными, периодическими и разовыми. Постоянные направления аналитической работы являются наиболее важными. Периодические и разовые направления аналитической работы характеризуются своей жесткой зависимостью от постоянных направлений. Промежутки времени, через которые проводятся исследования в области периодических направлений аналитической работы, всецело зависят от результатов анализа по постоянным направлениям. Разовые направления аналитической работы не только жестко зависят от постоянной аналитической работы, но и в подавляющем большинстве случаев являются следствием результатов таких исследований.

5.Что предусматривает аналитическое исследование источников конфиденциальной информации

Верный ответ: • выявление и классификацию существующих и возможных конкурентов и соперников фирмы, криминальных структур и отдельных преступных элементов, интересующихся фирмой; • выявление и классификацию максимально возможного числа источников конфиденциальной информации фирмы; • выявление, классификацию и ведение перечня (учетного аппарата) реального состава циркулирующей в фирме конфиденциальной информации (в разрезе источников, обеспечиваемых функций и видов работы, с указанием носителей – документов, дискет, файлов и т. д.); • изучение данных учета осведомленности сотрудников в тайне фирмы в разрезе каждого руководителя и сотрудника (в том числе технического и вспомогательного), т. е. изучение степени и динамики реального владения (в том числе случайного) сотрудниками конфиденциальной информацией; • изучение состава конфиденциальной информации в разрезе документов, т. е. изучение правильности расчленения тайны (конфиденциальной информации) между документами и определение избыточности ценной информации в документах; • учет и изучение выявленных внутренних и внешних, потенциальных и реальных (пассивных и активных) угроз каждому отдельному источнику информации, контроль процесса формирования канала несанкционированного доступа к информации; • ведение и анализ полноты перечня защитных мер, предпринятых по каждому источнику, и защитных мер, которые могут быть использованы при активных действиях злоумышленника, заблаговременное противодействие злоумышленнику.

6.Что предусматривает аналитическая работа с источником угрозы конфиденциальной информации

Верный ответ: • выявление и классификацию максимального состава источников угрозы конфиденциальной информации; • учет и изучение каждого отдельного субъективного внутреннего и внешнего источника, степени его опасности (анализ риска) при реализации угрозы; • разработку превентивных мероприятий по локализации и ликвидации объективных угроз.

7.Основным назначением всех аналитических методов является ….

Верный ответ: обработка полученных сведений, установление взаимосвязи между фактами, выявление значения этих связей и выработка конкретных предложений на основе достоверной и полной, аналитически обработанной информации.

8.Что является целью информационно-аналитической работы в области обеспечения информационной безопасности предприятия

Верный ответ: целью информационно-аналитической работы в области обеспечения информационной безопасности предприятия можно считать целенаправленный сбор, обработку и анализ информации, которая служит для выявления и нейтрализации реальных и потенциальных внутренних и внешних угроз предприятию.

9.Информационно-аналитическая работа в области безопасности, осуществляемая сотрудниками этого подразделения, должна включать в себя …

Верный ответ: Информационно-аналитическая работа в области безопасности, осуществляемая сотрудниками этого подразделения, должна включать в себя следующие направления: 1. Анализ объектов защиты информации, составляющих в целом защищаемый объект информатизации, которые включают в себя: - носители конфиденциальной информации; - хранилища и помещения, где хранятся и обрабатываются эти носители; - здание предприятия и при необходимости прилегающая к зданию территория. 2. Анализ внутренних угроз предприятия, включающий в себя следующие угрозы: - внутренние (возникающие в рамках самого предприятия) источники негативного воздействия на информацию; - причины, обстоятельства и условия такого воздействия; - каналы и методы несанкционированного доступа к информации со стороны внутренних источников воздействия; - социально-психологические аспекты внутренней среды предприятия,

которые влияют или могут повлиять на состояние защиты информации. 3. Анализ элементов комплексной системы защиты информации предприятия, таких, например, как: - виды средств защиты; - методы и средства защиты информации; - кадровое обеспечение защиты информации предприятия; - ресурсное обеспечение защиты информации предприятия.

10.К инструментальным средствам, ориентированным на реализацию собственно аналитических приложений в ИАСОБ относятся

Верный ответ: Средства: • статического анализа (традиционные регламентированные отчеты и диаграммы); • динамического анализа (динамические системы поддержки принятия решений); • моделирования и прогнозирования; • визуализации связей и отношений между объектами интересов (под которыми могут пониматься физические и юридические лица, события, явления, процессы и т.п.).

11.Какова суть технологий, применяемых в ИАСОБ стратегического уровня

Верный ответ: • формирование базы знаний (тематического каталога) с комбинацией "ручного" и автоматического способа формирования системы категорий; • навигацию по базе знаний, с добавлением или исключением из неё новых документов; • автоматизированный поиск взаимосвязей любых объектов, представляющих возможную угрозу (событий, людей, телефонных переговоров, адресов и т.п.); • визуализацию найденных в сложно структурированной информации возможных отношений и связей в графическом и табличном видах, а в ряде случаев их образное представление; • открытость архитектуры, с возможностью встраивания и/или наращивания новых информационных подсистем, с удалением или переконфигурацией уже имеющихся.

12.Назначение системы MaxPatrol 8

Верный ответ: Система MaxPatrol 8 предназначена для обеспечения контроля защищенности и соответствия стандартам безопасности информационных систем.

13.Механизм тестирования на проникновение (Pentest) MaxPatrol 8

Верный ответ: Режим тестирования на проникновение реализует проверки, типичные для сканера сетевого уровня: инвентаризационные, «баннерные» проверки, фаззинг, подбор учетных записей. Также в MaxPatrol 8 есть специализированные проверки для анализа защищенности веб-приложений и СУБД.

14.Механизм системных проверок (Audit) в MaxPatrol 8

Верный ответ: Режим системного сканирования позволяет провести инвентаризацию аппаратного и программного обеспечения, сбор конфигурационных параметров ОС, служб, СУБД, прикладных систем и средств защиты информации, выявить уязвимости, ошибки конфигурации и контролировать обновления.

15.Какие ключевые возможности имеет контроль защищенности и соответствия стандартам в MaxPatrol 8

Верный ответ: • Проактивная защита корпоративных ресурсов с помощью автоматического мониторинга ИБ; • Автоматизация процессов контроля соответствия отрасле¬вым и международным стандартам; • Оценка эффективности подразделений ИТ и ИБ с помощью расширяемого набора метрик безопасности и KPI; • Снижение затрат на аудит и контроль защищенности, подготовку ИТ и ИБ-проектов; • Автоматизация процессов инвентаризации ресурсов, управления уязвимостями, контроля соответствия политикам безопасности и контроля изменений; • Комплексный анализ сложных систем, включая сетевое оборудование Cisco, Nortel, Juniper, Huawei, платформ Windows, Linux, Unix, СУБД Microsoft SQL, Oracle, приложений Active Directory, Microsoft Exchange, Lotus, SAP/R3 и Web-службы собственной разработки; • Встроенная поддержка основных стандартов, таких как ГОСТ ИСО/МЭК 27001, SOX (Sarbanes-Oxley Act), PCI DSS (Payment Card Industry Data Security Standard), NSA (National Security Agency), NIST (National Institute of Standards and Technologies), CIS (Center for Internet Security); •

Максимальная автоматизация процессов снижает трудозатраты и позволяет оперативно контролировать состояние защищенности систем; • Поддержка базы знаний командой профессиональных экспертов.

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