ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«АКАДЕМИЯ ИНФОВОТЧ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0238DBC800C9B04981437026D4A6E6EAF2
Владелец: ХАРИТОНОВ СЕРГЕЙ ВЛАДИМИРОВИЧ
Действителен: с 29.11.2023 до 28.02.2025

Утверждена

Генеральный директор
С.В. Харитонов

МП

Дополнительная профессиональная программа
повышения квалификации
«Преподаватель по внедрению и использованию InfoWatch Traffic Monitor»

Форма обучения: заочная
с применением дистанционных образовательных технологий

Москва 2025

Оглавление

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая образовательная программа (далее – Программа) представляет собой совокупность требований, обязательных при реализации программы дополнительного профессионального образования повышения квалификации для сертификации преподавателей учебных заведений «Преподаватель по внедрению и использованию InfoWatch Traffic Monitor».

Программа разработана в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н (далее – Профстандарт), также на основании Приказа Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. № 499 г. Москва "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам" и на основании Федерального закона "Об образовании в Российской Федерации" от 29.12.2012 № 273-ФЗ.

Цели:

- формирование знаний и навыков по вопросам применения законодательства в сфере защиты информации от утечек, сбора и анализа требования к конфиденциальной информации, выявления потенциальных каналов утечки конфиденциальной информации и определения комплекса мер по предотвращению утечек
- практическая подготовка для обучения студентов выполнению работ по внедрению программных решений защиты от утечки данных (DLP-системы), разработке и реализации Политик защиты данных в системах защиты от утечки данных, а также оценки эффективности применения соответствующих Правил.

Категория слушателей:

- преподаватель
- старший преподаватель
- ведущий преподаватель
- доцент

Организационно-педагогические условия

Образовательный процесс осуществляется на основании учебного плана и регламентируется расписанием занятий для каждого слушателя.

Срок обучения: 101/4/1 (ак. час, нед., мес.).

Режим занятий: 93 академический час самостоятельного обучения, 6 академических часов практического занятия с использованием средств видеоконференцсвязи, 2 академических часа итоговой аттестации (зачета) с использованием средств видеоконференцсвязи.

Форма обучения: заочная с применением дистанционных образовательных технологий

Характеристика профессиональной деятельности слушателей

Область профессиональной деятельности слушателей:

- преподавание дисциплин, связанных с информационной безопасностью и защитой данных

Преподаватель готовит студентов к следующим видам деятельности: к участию в обеспечении безопасности информации с учетом требования эффективного функционирования автоматизированной системы, к участию в выявлении угроз безопасности информации в автоматизированных системах, к участию в принятии мер защиты информации при выявлении новых угроз безопасности информации.

Требования к результатам освоения дополнительной профессиональной образовательной программы

Специалист должен обладать общими компетенциями, включающими в себя способность:

- Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес.
- Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
- Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
- Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий.

Специалист должен обладать профессиональными компетенциями, соответствующими основным видам профессиональной деятельности:

- Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы.
- Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации.
- Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы.
- Выявление угроз безопасности информации в автоматизированных системах.
- Принятие мер защиты информации при выявлении новых угроз безопасности информации.
- Анализ недостатков в функционировании системы защиты информации автоматизированной системы.

- Устранение недостатков в функционировании системы защиты информации автоматизированной системы.

Требование к слушателям

Требования к образованию и обучению	Высшее профессиональное образование/Среднее профессиональное образование

Для реализации программы задействован следующий кадровый потенциал:

- **Преподаватели учебных дисциплин** - обеспечивается необходимый уровень компетенции преподавательского состава, включающий высшее образование в области соответствующей дисциплины программы или высшее образование в иной области и стаж преподавания по изучаемой тематике не менее трех лет; использование при изучении дисциплин программы эффективных методик преподавания, предполагающих выполнение слушателями практических заданий.

- **Административный персонал** - обеспечивает условия для эффективной работы педагогического коллектива, осуществляет контроль и текущую организационную работу.

- **Информационно-технологический персонал** - обеспечивает функционирование информационной структуры (включая ремонт техники, оборудования, макетов иного технического обеспечения образовательного процесса).

Содержание программы повышения квалификации определяется учебным планом и календарным учебным графиком программы дисциплин (модулей), требованиями к итоговой аттестации и требованиями к уровню подготовки лиц, успешно освоивших Программу.

Текущий контроль знаний проводится в форме наблюдения за работой обучающихся и контроля их активности на образовательной платформе, проверочного тестирования.

Промежуточный контроль знаний, полученных обучающимися посредством самостоятельного обучения (освоения части образовательной программы), проводится в виде тестирования.

Итоговая аттестация по Программе проводится в форме зачета и должна выявить теоретическую и практическую подготовку специалиста.

Слушатель допускается к итоговой аттестации после самостоятельного изучения дисциплин Программы в объеме, предусмотренном для обязательных внеаудиторных занятий и подтвердивший самостоятельное изучение сдачей тестов, а также лабораторного практикума.

Лица, освоившие Программу и успешно прошедшие итоговую аттестацию, получают удостоверение о повышении квалификации.

Оценочными материалами по Программе являются блоки контрольных вопросов по дисциплинам, формируемые образовательной организацией и используемые при текущем контроле знаний (тестировании), лабораторный практикум, теоретические вопросы и практические задания для итоговой аттестации.

Методическими материалами к Программе являются нормативные правовые акты и техническая документация по изучаемым программным продуктам, положения которых изучаются при освоении дисциплин Программы. Перечень методических материалов приводится в рабочей программе образовательной организации.

УЧЕБНЫЙ ПЛАН
ПО ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЕ
повышения квалификации

ПРЕПОДАВАТЕЛЬ ПО ВНЕДРЕНИЮ И ИСПОЛЬЗОВАНИЮ INFOWATCH TRAFFIC MONITOR

(профстандарт «Специалист по защите информации в автоматизированных системах» код B)

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоятельная работа)	Внеаудиторная (самостоятельная работа)	Промежуточная /итоговая аттестация	
1	DLP-системы как средство защиты от утечки данных	4,5	1,8	2,3	0,4	Тестирование
2	Архитектура и технологии InfoWatch Traffic Monitor	4,4	2,0	1,6	0,8	Тестирование
3	Развертывание InfoWatch Traffic Monitor	2,9	1,3	1,2	0,4	Тестирование
4	Развертывание InfoWatch Device Monitor	8,3	2,4	4,7	1,2	Тестирование
5	Администрирование InfoWatch Traffic Monitor	4,8	1,5	2,5	0,8	Тестирование
6	Обзор аналитических работ	6,5	2,5	3,0	1,0	Тестирование
7	Правовые и организационные аспекты легитимизации DLP-системы	3,8	1,3	2,0	0,5	Тестирование
8	Настройка и использование программных средств InfoWatch	10,1	5,6	4,0	0,5	Тестирование

9	**Подготовка и реализация Концепции Политики защиты данных**	**17,7**	**0,4**	**11,3**	**6,0**	**Лабораторный практикум**
10	**Внедрение и техническая поддержка Центра расследований InfoWatch**	**36,0**	**10,7**	**23,0**	**2,3**	**Тестирование**
11	**ИТОГОВАЯ АТТЕСТАЦИЯ**	**2,0**			**2,0**	**Зачет**
	Всего:	**101,0**	**29,5**	**55,6**	**15,9**	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
ПО
ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЕ
повышения квалификации

ПРЕПОДАВАТЕЛЬ ПО ВНЕДРЕНИЮ И ИСПОЛЬЗОВАНИЮ INFOWATCH TRAFFIC MONITOR

(профстандарт «Специалист по защите информации в автоматизированных системах» код B)

№ п/п	**Наименование разделов и дисциплин**	**Всего ак. часов**	**В том числе**			**Форма контроля**
			Видеолекции - внеаудиторная (самостоя-тельная работа)	**Внеауди-торная (самостоя-тельная работа)**	**Промеж у-точная /итоговая аттеста-ция**	
1	**DLP-системы как средство защиты от утечки данных**	**4,5**	**1,8**	**2,3**	**0,4**	**Тестирование**
1.1	Обзор возможностей, принципов работы и назначения DLP-систем	0,8	0,4	0,4		
1.2	Административно-организационные аспекты корпоративной защиты от внутренних угроз	0,8	0,4	0,4		
1.3	Интеграция DLP с другими системами	2,5	1,0	1,5		

1.4	Тестирование	0,4			0,4	
2	**Архитектура и технологии InfoWatch Traffic Monitor**	**4,4**	**2,0**	**1,6**	**0,8**	**Тестирование**
2.1	InfoWatch Traffic Monitor и комплементарные продукты	1,6	0,9	0,7		
2.2	Принципы работы InfoWatch Traffic Monitor	2,0	1,1	0,9		
2.3	Тестирование	0,8			0,8	
3	**Развертывание InfoWatch Traffic Monitor**	**2,9**	**1,3**	**1,2**	**0,4**	**Тестирование**
3.1	Подготовка к установке и настройка ОС	1,3	0,5	0,8		
3.2	Установка и первоначальная настройка	0,9	0,7	0,2		
3.3	Установка InfoWatch Data Analysis Service и его интеграция с InfoWatch Traffic Monitor	0,3	0,1	0,2		
3.4	Тестирование	0,4			0,4	
4	**Развертывание InfoWatch Device Monitor**	**8,3**	**2,4**	**4,7**	**1,2**	**Тестирование**
4.1	Развертывание InfoWatch Device Monitor for Windows	2,5	1,0	1,5		
4.2	Развертывание InfoWatch Device Monitor for Linux	2,0	0,7	1,3		
4.3	Обзор возможностей InfoWatch Device Monitor for Linux	2,6	0,7	1,9		
4.4	Тестирование	1,2			1,2	
5	**Администрирование InfoWatch Traffic Monitor**	**4,8**	**1,5**	**2,5**	**0,8**	**Тестирование**

5.1	Работа с компонентами	1,6	0,6	1,0		
5.2	Обслуживание сервера и настройка OCR	2,4	0,9	1,5		
5.3	Тестирование	0,8			0,8	
6	**Обзор аналитических работ**	**6,5**	**2,5**	**3,0**	**1,0**	**Тестирование**
6.1	Формирование плана аналитических работ и сбор требований	1,0	0,5	0,5		
6.2	Анализ данных в DLP-системе	3,5	1,5	2,0		
6.3	Подготовка данных и формирование Концепции Политики защиты данных	1,0	0,5	0,5		
6.4	Тестирование	1,0			1,0	
7	**Правовые и организационные аспекты легитимизации DLP-системы**	**3,8**	**1,3**	**2,0**	**0,5**	**Тестирование**
7.1	Нормативное обеспечение использования DLP-системы	1,7	0,7	1,0		
7.2	Организационное обеспечение использования DLP-системы	1,6	0,6	1,0		
7.3	Тестирование	0,5			0,5	
8	**Настройка и использование программных средств InfoWatch**	**10,1**	**5,6**	**4,0**	**0,5**	**Тестирование**
8.1	Настройка и использование InfoWatch Traffic Monitor	5,8	3,3	2,5		
8.2	Настройка и использование	3,8	2,3	1,5		

	InfoWatch Device Monitor					
8.3	Тестирование	0,5			0,5	
9	**Подготовка и реализация Концепции Политики защиты данных**	**17,7**	**0,4**	**11,3**	**6,0**	**Лабораторный практикум**
9.1	Подготовка Концепции Политики защиты данных	3,2	0,2	3,0		
9.2	Реализация Концепции Политики защиты данных	0,5	0,2	0,3		
9.3	Лабораторный практикум	14,0			8,0	
10	**Внедрение и техническая поддержка Центра расследований InfoWatch**	**36,0**	**10,7**	**23,0**	**2,3**	**Тестирование**
10.1	Центр расследований - единый интерфейс средств информационной безопасности InfoWatch	1,5	0,5	1,0		
10.2	Установка Центра расследований	4,0	1,0	3,0		
10.3	Общие функции Центра расследований	3,3	1,3	2,0		
10.4	InfoWatch Vision	2,7	0,7	2,0		
10.5	InfoWatch Activity Monitor	3,1	1,1	2,0		
10.6	InfoWatch Prediction	1,6	0,6	1,0		
10.7	InfoWatch Data Discovery	2,8	0,8	2,0		
10.8	InfoWatch Data Access Tracker	2,0	0,6	1,4		
10.9	InfoWatch Device Control	2,0	0,4	1,6		

10.10	Настройки Центра расследований	10,7	3,7	7,0		
10.11	Тестирование	2,3			2,3	
11	**ИТОГОВАЯ АТТЕСТАЦИЯ**	**2,0**			**2,0**	**Зачет**
	Всего:	**101,0**	**29,5**	**55,6**	**15,9**	**-**

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный график обучения является примерным, составляется и утверждается для каждого слушателя.

Срок освоения программы – 4 недели. Начало обучения – по мере набора слушателей. Примерный режим занятий: 2,0-4,5 академических часа в день (кроме практического занятия с использованием средств видеоконференцсвязи). Промежуточная и итоговые аттестации проводятся согласно графику.

№	Наименование модулей / дни	ВР	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	DLP-системы как средство защиты от утечки данных	СР	2,2	2,3																												
2	Архитектура и технологии InfoWatch Traffic Monitor	СР			2,2	2,2																										
3	Развертывание InfoWatch Traffic Monitor	СР					2,9																									
4	Развертывание InfoWatch Device Monitor	СР						4,0	4,3																							
5	Администрирование InfoWatch Traffic Monitor	СР								2,4	2,4																					
6	Обзор аналитических работ	СР										3,2	3,3																			
7	Правовые и организационные аспекты легитимизации DLP-системы	СР												2,0	1,8																	
8	Настройка и использование программных средств InfoWatch	СР														2,5	2,5	2,5	2,6													
9	Подготовка и реализация Концепции Политики защиты данных	СР																		3,7	4,0	4,0	6,0									
10	Внедрение и техническая поддержка Центра расследований InfoWatch	СР																						4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	
11	Итоговая аттестация	СР																														2,0

Рабочая программа учебной дисциплины «DLP-системы как средство защиты от утечки данных» (код В)

Цель: обеспечение глубоких знаний обучающихся в области назначения, возможностей и принципов работы системы защиты данных от утечек (DLP-системы).

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить возможности, процесс внедрения, а также интеграцию DLP с другими системами.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Теоретические основы проектирования системы корпоративной защиты от внутренних угроз.
- Порядок внедрения DLP-системы в корпоративную среду.
- Принципы работы инструментария API.

Уметь:

- Обосновывать необходимость использования DLP-системы в инфраструктуре.
- Проводить аудит корпоративной среды с целью внедрения DLP-системы.
- Определять технологии API, необходимые для внедрения DLP-системы.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4,5 академических часов; из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 4,5 академических часов.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттеста-ция	
1	**DLP-системы как средство защиты от утечки данных**	**4,5**	**1,8**	**2,3**	**0,4**	**Тестирование**
1.1	Обзор возможностей, принципов работы и назначения DLP-систем	0,8	0,4	0,4		
1.2	Административно-организационные аспекты корпоративной защиты от внутренних угроз	0,8	0,4	0,4		
1.3	Интеграция DLP с другими системами	2,5	1,0	1,5		
	Тестирование	0,4			0,4	

Тема 1.1. Обзор возможностей, принципов работы и назначения DLP-систем

- Безопасность IT-инфраструктуры.
- DLP-подход.

Тема 1.2. Административно-организационные аспекты корпоративной защиты от внутренних угроз

- Этапы внедрения DLP-системы.
- Pre-DLP, Post-DLP.

Тема 1.3. Интеграция DLP с другими системами

- PushAPI.
- DataExport API.
- REST API.

Рабочая программа учебной дисциплины «Архитектура и технологии InfoWatch Traffic Monitor» (код B)

Цель: обеспечение глубоких знаний обучающихся в области использования и внедрения и администрирования средств защиты от утечки данных: InfoWatch Traffic Monitor, InfoWatch Device Monitor, InfoWatch Data Discovery и InfoWatch Vision.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить процесс внедрения, администрирования и использования средств защиты от утечки данных: InfoWatch Traffic Monitor, InfoWatch Device Monitor, InfoWatch Data Discovery, InfoWatch Vision.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Теоретические основы проектирования системы корпоративной защиты от внутренних угроз с использованием InfoWatch Traffic Monitor и комплементарных продуктов.
- Инструментарий, технологии, область их применения и ограничения при формировании корпоративной защиты от внутренних угроз информационной безопасности на основе InfoWatch Traffic Monitor и комплементарных продуктов.

Уметь:

- Обосновывать необходимость использования DLP-системы InfoWatch Traffic Monitor и комплементарных продуктов.
- Работать с консолью InfoWatch Traffic Monitor, InfoWatch Device Monitor.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4,4 академических часа; из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 1,6 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоятельная работа)	Внеаудиторная (самостоятельная работа)	Промежуточная /итоговая аттестация	
2	**Архитектура и технологии InfoWatch Traffic Monitor**	**4,4**	**2,0**	**1,6**	**0,8**	**Тестирование**
2.1	InfoWatch Traffic Monitor и комплементарные продукты	1,6	0,9	0,7		
2.2	Принципы работы InfoWatch Traffic Monitor	2,0	1,1	0,9		
	Тестирование	0,8			0,8	

Тема 2.1. InfoWatch Traffic Monitor и комплементарные продукты

- Назначение и состав InfoWatch Traffic Monitor.
- InfoWatch Device Monitor возможности и принципы работы.
- InfoWatch Data Discovery возможности и принципы работы.
- InfoWatch Vision возможности и принципы работы.

Тема 2.2. Принципы работы InfoWatch Traffic Monitor

- Режимы перехвата InfoWatch Traffic Monitor.
- Архитектура системы InfoWatch Traffic Monitor.
- Технологии анализа контента.
- Создание политик защиты данных.

Рабочая программа учебной дисциплины «Развертывание InfoWatch Traffic Monitor» (код В)

Цель: обеспечение глубоких знаний обучающихся в области внедрения средств защиты от утечки данных: InfoWatch Traffic Monitor, InfoWatch Data Analysis Service.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить процесс внедрения средств защиты от утечки данных: InfoWatch Traffic Monitor, InfoWatch InfoWatch Data Analysis Service.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Теоретические основы проектирования системы корпоративной защиты от внутренних угроз с использованием InfoWatch Traffic Monitor и комплементарных продуктов.
- Инструментарий, технологии, область их применения и ограничения при формировании корпоративной защиты от внутренних угроз информационной безопасности на основе InfoWatch Traffic Monitor и комплементарных продуктов.

Уметь:

- Работать с консолью InfoWatch Traffic Monitor, InfoWatch Data Analysis Service.
- Развёртывать InfoWatch Traffic Monitor, InfoWatch Data Analysis Service.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2,9 академических часов; из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 1,2 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промеж у-точная /итогова я	

					аттеста-ция	
3	**Развертывание InfoWatch Traffic Monitor**	**2,9**	**1,3**	**1,2**	**0,4**	**Тестирование**
3.1	Подготовка к установке и настройка ОС	1,3	0,5	0,8		
3.2	Установка и первоначальная настройка	0,9	0,7	0,2		
3.3	Установка InfoWatch Data Analysis Service и его интеграция с InfoWatch Traffic Monitor	0,3	0,1	0,2		
	Тестирование	0,4			0,4	

Тема 3.1. Подготовка к установке и настройка ОС

- Подготовка к установке InfoWatch Traffic Monitor.
- Установка и настройка операционной системы Oracle Linux 7.9.
- Подготовка операционной системы РЕД ОС 7.3 для установки InfoWatch Traffic Monitor.
- Подготовка операционной системы Astra Linux 1.7.0 для установки InfoWatch Traffic Monitor.

Тема 3.2. Установка и первоначальная настройка

- Поэтапная установка InfoWatch Traffic Monitor в текстовом режиме.
- Первоначальная настройка InfoWatch Traffic Monitor.

Тема 3.3. Установка InfoWatch Data Analysis Service и его интеграция с InfoWatch Traffic Monitor

- Функциональные возможности InfoWatch Data Analysis Service.
- Аппаратные и программные требования InfoWatch Data Analysis Service.
- Подготовка сервера к sустановке/обновлению InfoWatch Data Analysis Service.
- Установка InfoWatch Data Analysis Service.
- Настройка InfoWatch Data Analysis Service.
- Удаление InfoWatch Data Analysis Service.
- Интеграция InfoWatch Traffic Monitor с InfoWatch Data Analysis Service.

Рабочая программа учебной дисциплины «Развертывание InfoWatch Device Monitor» (код B)

Цель: обеспечение глубоких знаний обучающихся в области внедрения средства защиты от утечки данных InfoWatch Device Monitor.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.

- Анализировать рабочую ситуацию, осуществлять текущий контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить процесс внедрения средств защиты от утечки данных InfoWatch Device Monitor.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Теоретические основы проектирования системы корпоративной защиты от внутренних угроз с использованием InfoWatch Traffic Monitor и его комплементарного продукта InfoWatch Device Monitor.
- Инструментарий, технологии, область их применения и ограничения при формировании корпоративной защиты от внутренних угроз информационной безопасности на основе InfoWatch Traffic Monitor и его комплементарного продукта InfoWatch Device Monitor.

Уметь:

- Работать с консолью InfoWatch Device Monitor.
- Развёртывать InfoWatch Device Monitor.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 8,3 академических часа; из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 4,7 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промеж у-точная /итогова я аттеста-ция	
4	**Развертывание InfoWatch Device Monitor**	**8,3**	**2,4**	**4,7**	**1,2**	**Тестирование**

4.1	Развертывание InfoWatch Device Monitor for Windows	2,5	1,0	1,5		
4.2	Развертывание InfoWatch Device Monitor for Linux	2,0	0,7	1,3		
4.3	Обзор возможностей InfoWatch Device Monitor for Linux	2,6	0,7	1,9		
	Тестирование	1,2			1,2	

Тема 4.1. Развертывание InfoWatch Device Monitor for Windows

- Аппаратные и программные требования для InfoWatch Device Monitor.
- Поэтапная установка InfoWatch Device Monitor.
- Настройка проверки сертификата сервера InfoWatch Traffic Monitor.
- Интеграция InfoWatch Device Monitor со службами каталогов.
- Установка агента на рабочую станцию.
- Конфигурирование и обслуживание InfoWatch Device Monitor.

Тема 4.2. Развертывание InfoWatch Device Monitor for Linux

- Аппаратные и программные требования для Device Monitor for Linux.
- Подготовка к установке сервера Device Monitor for Linux.
- Поэтапная установка web консоли Device Monitor for Linux.
- Поэтапная установка сервера Device Monitor for Linux.
- Установка агента Device Monitor for Linux.

Тема 4.3. Обзор возможностей InfoWatch Device Monitor for Linux

- Основные элементы интерфейса и меню пользователя Device Monitor for Linux.
- Настройки системы Device Monitor for Linux.
- Настройки продукта Device Monitor for Linux.
- Панель навигации Device Monitor for Linux.

Рабочая программа учебной дисциплины «Администрирование InfoWatch Traffic Monitor» (код В)

Цель: обеспечение глубоких знаний обучающихся в области администрирования средства защиты от утечки данных InfoWatch Traffic Monitor.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить процесс администрирования средства защиты от утечки данных InfoWatch Traffic Monitor.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Теоретические основы проектирования системы корпоративной защиты от внутренних угроз с использованием InfoWatch Traffic Monitor и комплементарных продуктов.
- Инструментарий, технологии, область их применения и ограничения при формировании корпоративной защиты от внутренних угроз информационной безопасности на основе InfoWatch Traffic Monitor и комплементарных продуктов.

Уметь:

- Работать с консолью InfoWatch Traffic Monitor.
- Выполнять обслуживание сервера InfoWatch Traffic Monitor.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4,8 академических часа; из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 2,5 академических часов.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промеж у-точная /итогова я аттеста-ция	
5	**Администрирование Traffic Monitor**	**4,8**	**1,5**	**2,5**	**0,8**	**Тестирование**
5.1	Работа с компонентами	1,6	0,6	1,0		
5.2	Обслуживание сервера и настройка OCR	2,4	0,9	1,5		
	Тестирование	0,8			0,8	

Тема 5.1. Работа с компонентами

- Диагностика работы.
- Администрирование работы компонент.
- Диагностика работы компонент.

Тема 5.2. Обслуживание сервера и настройка OCR

- Очистка места на сервере.
- Администрирование очередей.
- Настройка OCR-экстрактора Google Tesseract.
- Администрирование базы данных PostgreSQL.

Рабочая программа учебной дисциплины «Обзор аналитических работ» (код B)

Цель: обеспечение глубоких знаний обучающихся в области выявления информации, подлежащей защите, определения угроз, направленных на данную информацию и определения технологий, позволяющих предотвратить утечку информации.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить принципы выявления информации, подлежащей защите, технологии анализа контента, позволяющие предотвратить утечку информации, а также порядок формирования Политики защиты данных (как части Политики информационной безопасности).

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Методы сбора требований об информационных потоках организации.
- Методы выявления информации, подлежащей защите.
- Технологии анализа контента, реализованные в DLP-системе InfoWatch Traffic Monitor.
- Порядок подготовки Политики защиты данных.

Уметь:

- Определять оптимальный метод сбора требований исходя из ситуации.
- Комбинировать методы сбора требований с целью обеспечения полноты и оперативности получения информации.
- Определять информацию, подлежащую защите, порядок хранения и передачи информации, подлежащей защите.
- Определять угрозы защищаемой информации, а также технологии и способы предотвращения утечки защищаемой информации.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6,5 академических часов; из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 3,0 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	
6	**Обзор аналитических работ**	**6,5**	**2,5**	**3,0**	**1,0**	**Тестирование**
6.1	Формирование плана аналитических работ и сбор требований	1,0	0,5	0,5		
6.2	Анализ данных в DLP-системе	3,5	1,5	2,0		
6.3	Подготовка данных и формирование Концепции Политики защиты данных	1,0	0,5	0,5		
	Тестирование	1,0			1,0	

Тема 6.1. Формирование плана аналитических работ и сбор требований

- План аналитических работ.
- Сбор требований.
- Интервью.
- Опросный лист.
- Изучение документации.
- Определение чувствительной информации.

Тема 6.2. Анализ данных в DLP-системе

- Технологии анализа контента.
- Лингвистический анализ.
- Текстовые объекты.
- Эталонные документы.
- Бланки.
- Печати.
- Выгрузки из баз данных.
- Графические объекты.
- Автолингвист.

Тема 6.3. Подготовка данных и формирование Концепции Политики защиты данных

- Подготовка данных для формирования Концепции Политики защиты данных
- Формирование Концепции Политики защиты данных

Рабочая программа учебной дисциплины «Правовые и организационные аспекты легитимизации DLP-системы» (код В)

Цель: обеспечение глубоких знаний обучающихся в области нормативно-правового и организационного обеспечения использования системы защиты данных от утечек (DLP-системы) с учетом действующего Законодательства РФ.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить законодательство РФ в сфере защиты информации, в том числе от утечек, организационное обеспечение, направленное на информирование сотрудников об использовании в организации системы защиты от утечки данных, а также порядок привлечения к ответственности сотрудников, в случае выявления фактов утечки с учетом действующего Законодательства РФ.

В результате обучения дисциплине слушатели должны:

Знать:

- Основные нормативные документы РФ в сфере защиты информации.
- Порядок информирования сотрудников об использовании системы защиты от утечки данных.
- Порядок привлечения сотрудников к ответственности в случае выявления фактов утечки данных.

Уметь:

- Определять перечень и содержание локальных документов организации, направленных на защиту данных от утечек.
- Определять порядок действий для обеспечения легитимности использования системы защиты данных от утечек.
- Определять порядок действий по привлечению сотрудников к ответственности в случае выявления факта утечки защищаемой информации.

Тема 7.1. Нормативное обеспечение использования DLP-системы

- Конституция РФ.
- Федеральный закон 149 – ФЗ.
- Федеральный закон 152 – ФЗ.
- Федеральный закон 98 – ФЗ.
- Закон о государственной тайне.
- Нормативные документы регуляторов.
- Приказы ФСТЭК № 21 и №17.

Тема 7.2. Организационное обеспечение использования DLP-системы

- Личное и корпоративное.
- Рекомендации к легитимизации DLP.
- Нормативная документация.
- Специально-технические средства.
- Заключение по законодательству.
- Примеры судебных решений.
- Алгоритм увольнения сотрудника.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3,8 академических часа; из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 2,0 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	
7	**Правовые и организационные аспекты легитимизации DLP-системы**	**3,8**	**1,3**	**2,0**	**0,5**	**Тестирование**
7.1	Нормативное обеспечение использования DLP-системы	1,7	0,7	1,0		
7.2	Организационное обеспечение использования DLP-системы	1,6	0,6	1,0		
	Тестирование	0,5			0,5	

Рабочая программа учебной дисциплины «Настройка и использование программных средств InfoWatch» (код В)

Цель: обеспечение глубоких знаний обучающихся в области администрирования программных продуктов АО «ИнфоВотч», позволяющих обеспечить защиту от утечки данных.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить возможности программных продуктов АО «ИнфоВотч» , позволяющих обеспечить защиту от утечки данных.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Интерфейс систем InfoWatch Traffic Monitor и InfoWatch Device Monitor.
- Порядок администрирования InfoWatch Traffic Monitor в части работы со списками и элементами управления системой.
- Порядок наполнения технологий, создания Объектов защиты и Политик защиты данных в InfoWatch Traffic Monitor.
- Порядок формирования сводных отчетов, поиска событий и визуализации информации о событиях в InfoWatch Traffic Monitor.
- Порядок администрирования InfoWatch Device Monitor в части работы со списками, настройками системы, группами компьютеров и пользователей.
- Порядок создания Политик и Правил в InfoWatch Device Monitor.

Уметь:

- Проводить подготовительные настройки и создавать Политики защиты данных в InfoWatch Traffic Monitor.
- Формировать отчеты о событиях, зарегистрированных системой InfoWatch Traffic Monitor
- Выполнять действия по администрированию систем InfoWatch Traffic Monitor и InfoWatch Device Monitor.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 10,1 академических часа (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 4,0 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	
8	**Настройка и использование программных средств InfoWatch**	**10,1**	**5,6**	**4,0**	**0,5**	**Тестирование**
8.1	Настройка и использование InfoWatch Traffic Monitor	5,8	3,3	2,5		
8.2	Настройка и использование InfoWatch Device Monitor	3,8	2,3	1,5		
	Тестирование	0,5			0,5	

Тема 8.1. Настройка и использование InfoWatch Traffic Monitor

- Вводная часть по настройке и администрированию InfoWatch Traffic Monitor.
- Технологии "Категории и термины" и "Текстовые объекты".
- Технология "Эталонные документы".
- Технологии "Бланки" и "Печати".
- Технология "Выгрузки из БД".
- Технология "Графические объекты".
- Персоны.
- Периметры.
- Списки.
- Объекты защиты данных.
- Управление.
- Политики.
- Сводка.
- События.
- Отчеты.

Тема 8.2. Настройка и использование InfoWatch Device Monitor

- Вводная часть по InfoWatch Device Monitor.
- Начало работы с Консолью управления InfoWatch Device Monitor.
- Алгоритм подготовки к созданию политики в консоли InfoWatch Device Monitor.
- Раздел Ресурсы.
- Раздел Приложения.

- Раздел Категории сигнатур.
- Политики.
- Правило для Application Monitor.
- Правило для Clipboard Monitor.
- Правило для Cloud Storage Monitor.
- Правило для Device Monitor.
- Правило для File Monitor.
- Правило для FTP Monitor.
- Правило для HTTP(S) Monitor.
- Правило для IM Client Monitor.
- Правило для Keyboard Monitor.
- Правило для Mail Monitor.
- Правило для Network Monitor.
- Правило для Print Monitor.
- Правило для ScreenShot Control Monitor.
- Правило для ScreenShot Monitor.
- Правило для File Operation Monitor.
- Раздел Группы сотрудников и как на них назначить политику.
- Раздел Группы компьютеров и как на них назначить политику.
- Белые списки.
- Настройки.
- Установка агента.

Рабочая программа учебной дисциплины «Подготовка и реализация Концепции Политики защиты данных» (код B)

Цель: обеспечение глубоких знаний обучающихся в области разработки и реализации Политики защиты данных, направленной на предотвращение утечки защищаемой информации.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям получить практические навыки разработки и реализации Политики защиты данных, направленной на предотвращение утечки защищаемой информации.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Порядок анализа предоставленных документов.
- Порядок определения технологии анализа контента исходя из характера и требований к защищаемой информации.
- Порядок определения объектов защиты исходя из выбранных технологий анализа контента, а также характера и требований к защищаемой информации.
- Порядок определения доверенных отправителей и получателей защищаемой информации.
- Порядок определения Политик защиты данных и правил реагирования системы.

Уметь:

- Формировать Политику защиты данных.
- Настраивать технологии анализа контента InfoWatch Traffic Monitor.
- Создавать Объекты защиты.
- Создавать Политики защиты данных InfoWatch Traffic Monitor.
- Создавать Политики InfoWatch Device Monitor.
- Оценивать результаты работы реализованных Политик и выполнять их доработку.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 17,7 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 11,3 академических часа, практическое занятие (лабораторный практикум) с использованием средств видеоконференцсвязи - 6 часов.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	
9	**Подготовка и реализация Концепции Политики защиты данных**	**17,7**	**0,4**	**11,3**	**6,0**	**Лабораторный практикум**
9.1	Подготовка Концепции Политики защиты данных	3,2	0,2	3,0		
9.2	Реализация Концепции Политики защиты данных	0,5	0,2	0,3		

9.3	Лабораторный практикум	14,0		8,0	6,0	

Тема 9.1. Подготовка Концепции Политики защиты данных

- Этапы подготовки Концепции.
- Выявление требований и подготовка данных.
- Формирование концепции.

Тема 9.2. Реализация Концепции Политики защиты данных

- Используемые технологии анализа.
- Объекты защиты.
- Списки отправителей/получателей.
- Политики защиты данных.

Рабочая программа учебной дисциплины «Внедрение и техническая поддержка Центра расследований InfoWatch» (код B)

Цель: обеспечение глубоких знаний обучающихся в области использования, внедрения и администрирования средств защиты от утечки данных: InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Prediction и InfoWatch Activity Monitor, InfoWatch Data Access Tracker, InfoWatch Device Control.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить процесс внедрения, администрирования и использования средств защиты от утечки данных: InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Activity Monitor, InfoWatch Prediction, InfoWatch Data Access Tracker, InfoWatch Device Control.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Назначение и возможности продуктов, входящих в Центр расследований: InfoWatch Vision, InfoWatch Activity Monitor, InfoWatch Prediction, InfoWatch Data Discovery, InfoWatch Data Access Tracker, InfoWatch Device Control;
- Порядок работы с общими разделами Центра расследований.

- Порядок работы с продуктами, входящими в Центр расследований: InfoWatch Vision, InfoWatch Activity Monitor, InfoWatch Prediction, InfoWatch Data Discovery, InfoWatch Data Access Tracker, InfoWatch Device Control;
- Возможности настройки Центра расследований.

Уметь:

- Проводить расследования инцидентов внутренней информационной безопасности с использованием Центра расследований.
- Администрировать Центр расследований.
- Работать с консолью Центр расследований.
- Развертывать InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Activity Monitor, InfoWatch Prediction, InfoWatch Data Access Tracker, InfoWatch Device Control.
- Конфигурировать и обслуживать InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Activity Monitor, InfoWatch Prediction, InfoWatch Data Access Tracker, InfoWatch Device Control.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 36,0 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 23,0 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоятельная работа)	Внеаудиторная (самостоятельная работа)	Промежуточная /итоговая аттестация	
10	**Внедрение и техническая поддержка Центра расследований InfoWatch**	**36,0**	**10,7**	**23,0**	**2,3**	**Тестирование**
10.1	Центр расследований - единый интерфейс средств информационной безопасности InfoWatch	1,5	0,5	1,0		
10.2	Установка Центра расследований	4,0	1,0	3,0		
10.3	Общие функции Центра расследований	3,3	1,3	2,0		
10.4	InfoWatch Vision	2,7	0,7	2,0		

10.5	InfoWatch Activity Monitor	3,1	1,1	2,0		
10.6	InfoWatch Prediction	1,6	0,6	1,0		
10.7	InfoWatch Data Discovery	2,8	0,8	2,0		
10.8	InfoWatch Data Access Tracker	2,0	0,6	1,4		
10.9	InfoWatch Device Control	2,0	0,4	1,6		
10.10	Настройки Центра расследований	10,7	3,7	7,0		
	Тестирование	2,3			2,3	

Тема 10.1. Центр расследований - единый интерфейс средств информационной безопасности InfoWatch

- Платформа для установки продуктов InfoWatch: Vision, Activity Monitor, Prediction, Data Discovery, Data Access Tracker, Device Control.
- Назначение и возможности продуктов InfoWatch: Vision, Activity Monitor, Prediction, Data Discovery, Data Access Tracker, Device Control.
- Обзор консоли управления Центра расследований.

Тема 10.2. Установка Центра расследований

- Аппаратные и программные требования для установки Центра расследований.
- Установка Центра расследований на Red Hat Enterprise и Oracle Linux.
- Установка Центра расследований на Astra Linux.
- Импорт конфигурации в Traffic Monitor для работы Prediction.
- Настройка контроллера домена и учётной записи Active Directory для работы Data Access Tracker.
- Установка Модуля контентного анализа.
- Установка IW Device Monitor for Windows.
- Установка агента IW Device Monitor for Windows.
- Поэтапная установка Device Monitor for Linux.
- Установка агента Device Monitor for Linux.

Тема 10.3. Общие функции Центра расследований

- Главная.
- Раздел События.
- Раздел Персоны.
- Раздел Расследования.
- Раздел Отчеты.

Тема 10.4. InfoWatch Vision

- Раздел Аналитика - Статистика нарушений.
- Виджеты Аналитика - Статистика нарушений.

- Работа с разделом Аналитика - Статистика нарушений Добавление и удаление виджетов.
- Настройка виджетов.
- Раздел Аналитика - Граф связей.
- Элементы Графа связей.
- Типы событий на Графе связей.
- Работа с Графом связей.
- Режим редактирования Графа связей.

Тема 10.5. InfoWatch Activity Monitor

- Раздел Аналитика - Статистика активности.
- Работа с разделом Аналитика - Статистика активности.
- Виджеты.
- Статистика Активности.
- Раздел Мониторинг.
- Наблюдение.
- Таймлайн.
- События Активности.
- Действие с файлами.
- Снимки экрана.
- Аудиозаписи.
- Видеозаписи.

Тема 10.6. InfoWatch Prediction

- Раздел Риски.
- Группы рисков и паттерны.
- Приоритеты источника данных.
- Работа с рисками.
- Контроль рисков.

Тема 10.7. InfoWatch Data Discovery

- Раздел Хранение файлов.
- Подготовка к созданию задачи.
- Создание задачи.
- Добавление Хоста.
- Определение путей сканирования.
- Панель навигации.
- Запуск задачи.
- Результат.
- Информация о файлах.
- Похожие файлы.
- Дубликаты файлов.

Тема 10.8. InfoWatch Data Access Tracker

- Раздел Инфраструктура.
- Аудит службы каталогов.
- Контроль изменения групп.

Тема 10.9. InfoWatch Device Control

- Раздел Устройства.
- События использования.
- Правила.
- Группы устройств.

Тема 10.10. Настройки Центра расследований

- Первоначальная настройка Центра расследований.
- Первоначальная настройка Device Monitor.
- Настройки системы.
- Настройки продуктов.
- Настройка правил Device Monitor для Activity Monitor.

ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

Формы аттестации

Для проведения промежуточной и итоговой аттестации программы разработан фонд оценочных средств по Программе, являющийся неотъемлемой частью учебно-методического комплекса.

Объектами оценивания выступают:

- степень освоения теоретических знаний;
- уровень овладения практическими умениями и навыками по всем видам учебной работы, активность на занятиях.

Текущий контроль знаний проводится в форме наблюдения за работой обучающихся и контроля их активности на образовательной платформе, проверочного тестирования.

Промежуточная аттестация - оценка качества усвоения обучающимися содержания учебных блоков непосредственно по завершении их освоения, проводимая в форме зачета посредством тестирования и лабораторного практикума.

Итоговая аттестация - процедура, проводимая с целью установления уровня знаний, обучающихся с учетом прогнозируемых результатов обучения и требований к результатам освоения образовательной программы. Итоговая аттестация обучающихся осуществляется в форме зачета посредством тестирования.

Слушатель допускается к итоговой аттестации после изучения тем образовательной программы в объеме, предусмотренном для лекционных и практических занятий.

Лицам, освоившим образовательную программу повышения квалификации «Преподаватель по внедрению и использованию InfoWatch Traffic Monitor» и успешно прошедшим итоговую аттестацию, выдается **удостоверение о повышении квалификации**

установленного образца с указанием названия программы, календарного периода обучения, длительности обучения в академических часах.

Для аттестации обучающихся на соответствие их персональных достижений требованиям соответствующей ОП созданы фонды оценочных средств, включающие типовые задания, тесты и методы контроля, позволяющие оценить знания, умения и уровень приобретенных компетенций.

Фонды оценочных средств соответствуют целям и задачам программы подготовки специалиста, учебному плану и обеспечивают оценку качества общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся.

Критерии оценки обучающихся

Предмет оценивания (компетенции)	**Объект оценивания (навыки)**	**Показатель оценки (знания, умения)**
Специалист должен обладать общими компетенциями (ОК), включающими в себя способность: - Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес. - Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. - Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. - Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач,	**Специалист должен обладать профессиональными компетенциями (ПК), соответствующими основным видам профессиональной деятельности:** - Выполнение установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы. - Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации. - Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации	**Знания:** - Принципы формирования политики информационной безопасности в автоматизированных системах. - Программно-аппаратные средства защиты информации автоматизированных систем. - Принципы организации и структура систем защиты программного обеспечения автоматизированных систем. - Нормативные правовые акты в области защиты информации. - Организационные меры по защите информации. **Умения:** - Формировать политику безопасности программных компонентов автоматизированных систем. - Регистрировать события, связанные с защитой информации в автоматизированных системах. - Анализировать события, связанные с защитой

профессионального и личностного развития. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. Ориентироваться в условиях частой смены технологий в профессиональной деятельности. Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий.	автоматизированной системы. Выявление угроз безопасности информации в автоматизированных системах. Принятие мер защиты информации при выявлении новых угроз безопасности информации. Анализ недостатков в функционировании системы защиты информации автоматизированной системы. Устранение недостатков в функционировании системы защиты информации автоматизированной системы.	информации в автоматизированных системах. Классифицировать и оценивать угрозы информационной безопасности. Контролировать события безопасности и действия пользователей автоматизированных систем.

Оценка качества освоения учебных модулей проводится в процессе промежуточной аттестации в форме тестирования и прохождения лабораторного практикума.

Оценка	Критерии оценки
Зачтено	Оценка **«Зачтено»** выставляется слушателю, если он твердо знает материал курса, грамотно и по существу использует его, не допуская существенных неточностей в ответе на тестовые вопросы. Не менее 70% правильных ответов при решении тестов. Не более 2-х ошибок при решении лабораторного практикума.
Не зачтено	Оценка **«Не зачтено»** выставляется слушателю, который не знает значительной части программного материала, допускает существенные ошибки. Менее 70% правильных ответов при решении тестов. Более 2-х ошибок при решении лабораторного практикума.

Оценка качества освоения учебной программы проводится в процессе итоговой аттестации в форме ответов на теоретические вопросы и решения практических задач.

Оценка (стандартная)	**Требования к знаниям**
Зачтено	Оценка **«Зачтено»** выставляется слушателю, продемонстрировавшему твердое и всестороннее знание материала, умение применять полученные в рамках занятий практические навыки и умения, знание и умение применять теоретические положения при решении практических вопросов, владеет необходимыми навыками и приемами их выполнения. Достижения за период обучения и результаты промежуточной аттестации демонстрировали отличный уровень знаний и умений слушателя. Не менее 70% правильных ответов на теоретические вопросы и правильных решений практических задач.
Не зачтено	Оценка **«Не зачтено»** выставляется слушателю, который в недостаточной мере овладел теоретическим материалом по дисциплине, допустил ряд грубых ошибок при выполнении практических заданий, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно, а также не выполнил требований, предъявляемых к промежуточной аттестации. Достижения за период обучения и результаты промежуточной аттестации демонстрировали неудовлетворительный уровень знаний и умений слушателя. Менее 70% правильных ответов на теоретические вопросы и правильных ответов при решении практических задач.

Фонд оценочных средств

Оценочные материалы

ТЕСТОВЫЕ ВОПРОСЫ

Дисциплина «DLP-системы как средство защиты от утечки данных»

1. Может ли DLP-система реагировать на внешние угрозы?
   - может обнаруживать и предотвращать.
   - может обнаруживать и информировать о них офицера безопасности.
   - может предотвращать и информировать об этом офицера безопасности.
   - не может.

2. Что является объектом защиты в DLP-системе?
   - информация.
   - технологии.
   - серверы.
   - базы данных.

3. Расположите в правильном порядке этапы внедрения DLP-системы:
   - pre-DLP.
   - развёртывание DLP-системы.
   - DLP.
   - post-DLP.

4. В чём состоит принцип работы программного интерфейса PushAPI?
   - сторонние компоненты самостоятельно формируют события перехвата данных и передают их в InfoWatch Traffic Monitor.
   - InfoWatch Traffic Monitor самостоятельно запрашивает события у сторонних систем
   - внешние системы получают данные из InfoWatch Traffic Monitor.
   - InfoWatch Traffic Monitor передаёт данные во внешние системы.

5. В чём состоит принцип работы программного интерфейса DataExport API?
   - внешние системы получают данные из InfoWatch Traffic Monitor.
   - InfoWatch Traffic Monitor передаёт данные во внешние системы.
   - сторонние компоненты самостоятельно формируют события перехвата данных и передают их в InfoWatch Traffic Monitor.
   - InfoWatch Traffic Monitor самостоятельно запрашивает события у сторонних систем.

6. В чём состоит принцип работы программного интерфейса REST API?
   - сторонние компоненты самостоятельно формируют данные и передают их в InfoWatch Traffic Monitor.
   - InfoWatch Traffic Monitor запрашивает данные у сторонних компонент.
   - внешние системы получают данные из InfoWatch Traffic Monitor.
   - InfoWatch Traffic Monitor передаёт данные во внешние системы.

Дисциплина «Архитектура и технологии InfoWatch Traffic Monitor»

1. Какая задача решается с помощью InfoWatch Data Discovery?
   - Получение данных находящихся в покое: из сетевых хранилищ, Share Point и с локальных дисков рабочих станций пользователей.
   - Визуальный анализ и формирование представления данных в любом разрезе.
   - Получение данных с рабочих станций пользователей.
   - Получение данных с почтового сервера, Proxy сервера и SPAN порта, а так же, от других систем. Настройка, обработка, анализ и применение политик защиты данных.

2. Какие технологии анализа работают непосредственно на агенте InfoWatch Device Monitor? (выберите несколько вариантов ответа)
   - Лингвистический анализ.
   - Детектор текстовых объектов.
   - Детектор эталонных документов.
   - Детектор заполненных бланков.
   - Детектор эталонных печатей.
   - Детектор выгрузок из баз данных.
   - Детектор графических объектов.
   - Автолингвист.

3. Какой почтовый сервер устанавливается совместно с InfoWatch Traffic Monitor и используется для отправки сообщений получателю или следующему relay-серверу в почтовой системе?
   - Microsoft Exchange Server.
   - Sendmail.
   - Postfix.
   - Exim.
   - Qmail.

- Apache James server.

4. По каким протоколам может быть перехвачена информация, поступающая со SPAN порта соответствующего сетевого оборудования на сервер InfoWatch Traffic Monitor? (выберите несколько вариантов ответа)
   - HTTP.
   - HTTPS.
   - FTP.
   - FTPS.
   - SMTP.
   - POP3.
   - IMAP.
   - NRPC.
   - NRPC/SSL.
   - MAPI.
   - XMPP.

5. Какая компонента InfoWatch Traffic Monitor отвечает за прием данных со SPAN порта?
   - iw_sniffer.
   - iw_capstack.
   - iw_messed.
   - iw_analysis.

6. Какая компонента InfoWatch Traffic Monitor отвечает за прием данных с Proxy сервера?
   - iw_proxy_smtp.
   - iw_proxy_http.
   - iw_icap.
   - iw_xapi.

7. Какую функцию выполняет компонента iw_warpd?
   - извлекает данные из контейнеров, вложенных в перехваченные объекты.
   - определяет наличие объекта защиты и добавляет объекту соответствующие атрибуты.
   - запускает по порядку все технологии анализа, которые установлены в системе.
   - применяет политики к перехваченным объектам.

8. При реализации филиальной структуры, какой сервер может быть только один (без вспомогательной или дополнительной ноды)?
   - База данных InfoWatch Traffic Monitor.
   - InfoWatch Traffic Monitor.
   - Microsoft Active Directory.
   - InfoWatch Device Monitor.
   - База данных InfoWatch Device Monitor.

9. Как InfoWatch Traffic Monitor получает объекты от InfoWatch Device Monitor и InfoWatch Data Discovery, а также внешних систем?
   - через адаптеры по thrift-интерфейсу.
   - по протоколу ICAP.
   - по протоколу MIME.
   - по SPAN протоколу.

10. К какому внутреннему формату приводятся объекты в InfoWatch Traffic Monitor?
    - XML+DAT.
    - MIME.
    - EML.
    - XML.
    - DAT.
    - EML+ DAT.

Дисциплина «Развертывание InfoWatch Traffic Monitor»

1. Какая программа используется для получения сведений о статусе процессов InfoWatch Traffic Monitor, сбора статистики и отправки уведомлений администратору сервера?
    - Zabbix.
    - Nagios.
    - Sensu.
    - Icinga.

2. Автоматическое удаление событий из БД…
    - включено по умолчанию и может быть изменено в процессе установки, период хранения может быть установлен индивидуально для событий разного типа (с нарушениями, без нарушений, хранение скриншотов).
    - включено по умолчанию и не может быть изменено в процессе установки.
    - выключено по умолчанию и не может быть изменено в процессе установки.
    - включено по умолчанию и может быть изменено в процессе установке, период хранения устанавливается одинаковым для всех типов событий (с нарушениями, без нарушений, хранение скриншотов).

3. Параметр установки InfoWatch Traffic Monitor «Daily tablespace paths» определяет…
    - путь к диску хранения данных ежедневного табличного пространства.
    - путь к диску хранения данных основного табличного пространства.
    - количество путей для файлов ежедневных табличных пространств.
    - путь к диску хранения файлов архивированных табличных пространств.

4. Какая децентрализованная отказоустойчивая система обнаружения сервисов (Service Discovery) используется в InfoWatch Traffic Monitor для регистрации сервисов, мониторинга доступности и обнаружения компонент?
    - Consul.
    - Redis.
    - Etcd.
    - ZooKeeper.
    - Doozerd.

5. Какие предлагаются варианты указания NTP-сервера при установке InfoWatch Traffic Monitor? (выберите несколько вариантов ответа)
    - Use system NTP-server.
    - DHCP.
    - Set manually.
    - PROXY.

Дисциплина «Развертывание InfoWatch Device Monitor»

1. На какие операционные системы может быть установлен агент InfoWatch Device Monitor версии 7.13? (выберите несколько вариантов ответа)
   - Microsoft Windows 7 Service Pack 1 и выше.
   - Microsoft Windows Server 2008 R2 и выше.
   - РЕД ОС 7.3.
   - Astra Linux Special Edition 1.7 в редакциях "Орел", "Воронеж" и "Смоленск".
   - Альт Рабочая станция 10.
   - MacOS 10.14 и выше.
   - Red Hat Enterprise Linux 7.0 и выше.

2. Ключ шифрования (ключ защищенного канала) InfoWatch Device Monitor…
   - создается при установке Основного сервера, далее указывается при установке Вспомогательных серверов.
   - создается отдельно для каждой ноды сервера InfoWatch Device Monitor, т.е. отдельно для Основного сервера и каждого из Вспомогательных серверов.
   - запрашивается в службе технической поддержки компании «ИнфоВотч» и указывается при установке как Основного, так и Вспомогательных серверов InfoWatch Device Monitor.
   - запрашивается в службе технической поддержки компании «ИнфоВотч» отдельно для каждой ноды сервера InfoWatch Device Monitor, т.е. отдельно для Основного сервера и каждого из Вспомогательных серверов.

3. Ключ шифрования (ключ защищенного канала) InfoWatch Device Monitor необходим для…
   - обнаружения сервером агентов, ранее установленных на рабочих станциях.
   - шифрования данных, которые передаются с сервера InfoWatch Device Monitor на сервер InfoWatch Traffic Monitor.
   - шифрования данных, которые передаются с сервера InfoWatch Traffic Monitor на сервер InfoWatch Device Monitor.
   - шифрования данных, которые передаются между агентом InfoWatch Device Monitor и сервером InfoWatch Device Monitor.
   - обнаружения агентами всех доступных серверов в своем окружении.
   - шифровании данных, которые передаются между сервером InfoWatch Device Monitor и базой данных.

4. Как получить сертификат web-сервера InfoWatch Traffic Monitor?
   - запросить в службе технической поддержки.
   - скопировать с сервера, где установлен InfoWatch Traffic Monitor файл /opt/iw/tm5/etc/web.conf.
   - на сервере, где установлен InfoWatch Traffic Monitor открыть файл /opt/iw/tm5/etc/xapi.conf, в секции "ThriftServers -> xapi", в параметре "TrustedCertificatesPath" будет указано расположение и имя файла с сертификатом web-сервера InfoWatch Traffic Monitor.
   - выполнить экспорт файла сертификата из web-браузера где открыта консоль управления InfoWatch Traffic Monitor.

5. Конфигурация Блокады приложений...
   - настраивается специалистом исключительно самостоятельно.

- загружается из соответствующего файла, который входит в поставку системы.
- загружается из соответствующего файла, который необходимо запросить в технической поддержке.
- может быть загружена из соответствующего файла, который приобретается дополнительно.

6. Какая колоночная аналитическая СУБД используется для работы web-консоли InfoWatch Device Monitor for Linux?
   - Vertica.
   - ParAccel.
   - ClickHouse.
   - Greenplum Database.
   - Sybase IQ.
   - Kognito.

7. Какое средство управления кластером контейнеров используется для работы web-консоли InfoWatch Device Monitor for Linux?
   - Kubernetes.
   - OpenShift.
   - Salt.
   - Vagrant.
   - Rancher.

8. Какая реляционная СУБД используется для работы сервера InfoWatch Device Monitor for Linux?
   - PostgresSQL.
   - Oracle.
   - DB2.
   - MS SQL Server.
   - MySQL.

9. Как получить токен шифрования трафика обмена данными между сервером InfoWatch Device Monitor for Linux и сервером InfoWatch Traffic Monitor?
   - запросить в службе технической поддержки компании «ИнфоВотч».
   - приобрести дополнительно у компании «ИнфоВотч».
   - скопировать из файла token.conf.
   - скопировать через web-консоль InfoWatch Traffic Monitor: Управление -> Плагины -> Device Monitor -> Токены -> Скопировать токен.

10. Как указать к какому серверу InfoWatch Device Monitor for Linux должен подключаться агент InfoWatch Device Monitor for Linux в случае его локальной установки на рабочей станции?
    - указать ip адрес или доменное имя сервера InfoWatch Device Monitor for Linux в процессе интерактивной установки агента.
    - указать ip адрес или доменное имя сервера InfoWatch Device Monitor for Linux в качестве параметра при запуске скрипта установки агента.
    - указать ip адрес или доменное имя сервера InfoWatch Device Monitor for Linux через web-консоль управления настройками агента InfoWatch Device Monitor for Linux после его установки.
    - никак не указывать, сервер InfoWatch Device Monitor for Linux самостоятельно обнаруживает компьютеры, на которые установлен агент.

11. Какой браузер/браузеры рекомендуется использовать для работы с web-консолью InfoWatch Device Monitor for Linux?
    - Амиго.
    - Google Chrome.
    - Яндекс.Браузер.
    - Opera.
    - MS Edge.
    - Orbitum.

12. Политики InfoWatch Device Monitor for Linux могут быть назначены…
    - только группе компьютеров.
    - группе компьютеров или группе пользователей.
    - группе компьютеров или отдельному компьютеру, не входящему ни в одну группу.
    - только группе пользователей.

13. В Группу компьютеров по умолчанию входят компьютеры…
    - впервые зарегистрированные в InfoWatch Device Monitor.
    - исключенные из всех прочих групп компьютеров.
    - добавленные в Microsoft Active Directory.
    - добавленные администратором системы вручную.

14. Какие действия допустимы для предустановленной учетной записи «Officer»? **(выберите несколько вариантов ответа)**
    - смена пароля.
    - изменение имени пользователя.
    - добавление контактов.
    - изменение языка консоли.
    - изменение роли.
    - удаление.

15. При потери рабочей станцией связи Агента с сервером InfoWatch Device Monitor for Linux…
    - теневые копии событий будут сохранятся на рабочей станции, при восстановлении соединения они будут переданы на сервер, если свободное место на диске закончится, то продолжение выполнения операций на рабочей станции будет разрешено или заблокировано в зависимости от сделанных настроек Агента.
    - рабочая станция будет заблокирована до восстановления связи.
    - рабочая станция продолжить функционировать в обычном режиме без передачи или сохранения информации о событиях.
    - теневые копии событий будут сохранятся на рабочей станции, при восстановлении соединения они будут переданы на сервер, если свободное место на диске закончится, то рабочая станция продолжить функционировать в обычном режиме без передачи или сохранения информации о событиях.

Дисциплина «Администрирование InfoWatch Traffic Monitor»

1. Какая команда выполняет «мягкую» остановку процесса cas?
    - iwtm kill cas.

- iwtm remove cas.
- iwtm stop cas.
- iwtm delete cas.
- iwtm disable cas.

2. Выполнение команды iwtm status cas отобразило статус компоненты «inactive (dead) loaded (enabled)» это означает что…
   - компонента загружена и запущена.
   - компонента загружена, но не запущена.
   - компонента не загружена и не запущена.
   - компонента не доступна для загрузки и запуска.

3. Какие опции доступны для команды «iwtm»? (выберите несколько вариантов ответа)
   - reload.
   - reboot.
   - test.
   - disable.
   - run.
   - activate.
   - shutdown.

4. В каком каталоге находятся конфигурационные файлы системы InfoWatch Traffic Monitor?
   - /etc.
   - /opt/iw/tm5/bin.
   - /opt/iw/tm5/etc.
   - /opt/iw/tm5/queue/.
   - /var/log/infowatch/.

5. В каком каталоге находятся очереди обработки объектов системы InfoWatch Traffic Monitor?
   - /opt/iw/tm5/queue/.
   - /opt/iw/tm5/etc.
   - /opt/iw/tm5/bin.
   - /u01/postgres.
   - /u02/pgdata.

6. Какой скрипт позволяет удалить временные файлы InfoWatch Traffic Monitor?
   - opt/iw/tm5/bin/clean_temporary_files.sh.
   - /opt/iw/tm5/bin/iw_qtool.
   - /opt/iw/tm5/bin/iw_vademcum.
   - /opt/iw/tm5/bin/iw_tech_tools.

7. Какие опции доступны для скрипта «iw_qtool»? (выберите несколько вариантов ответа))
   - move.
   - remove.
   - delete.
   - clean.
   - put.
   - stat.

- erase.
- load.

8. Как вывести на экран в реальном времени информацию о работе базы данных PostgreSQL?
   - tail –f /u01/postgres/pg_log/postgresql.log.
   - tail -f /var/log/messages.
   - tail -f /var/log/syslog.
   - tail -f /var/log/pgagent-9.6.log.

9. Какую команду необходимо выполнить для того, чтобы установить срок хранения событий с нарушениями равным 60 дней для СУБД Postgres?
   - ./dbconf-iwdrop-postgres.sh set violation 60.
   - ./dbconf-iwdrop-postgres.sh set noviolation 60.
   - ./dbconf-iwdrop-postgres.sh set other 60.
   - ./dbconf-iwdrop-postgres.sh set screenshot 60.

10. В каком файле устанавливается минимальный и максимальный размер растровых изображений (графических файлов), к которым будет применяться OCR Google Tesseract?
    - /opt/iw/tm5/etc/image2text_ts.conf.
    - /opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml.
    - /opt/iw/tm5/etc/sample_compiler.conf.
    - /opt/iw/tm5/etc/warpd.conf.

Дисциплина «Обзор аналитических работ»

1. Отметьте достоинства метода выявления требований «Интервью» (выберите несколько вариантов ответа):
   - произвольная последовательность вопросов.
   - использование вспомогательных материалов.
   - быстрое получение первичной информации.
   - минимальные затраты времени на общение.
   - возможность получения одинаковых ответов от интервьюируемых.

2. Отметьте способы, с помощью которых в процессе интервью можно получить наиболее полную информацию (выберите несколько вариантов ответа):
   - менять порядок заготовленных вопросов, исключать одни вопросы и добавлять другие.
   - менять формулировку вопроса если интервьюируемому вопрос не понятен.
   - вести заметки.
   - предварительно выслать перечень вопросов.
   - четко следовать подготовленному плану интервью.
   - строго соблюдать порядок и формулировку заготовленных вопросов.
   - назначить удобное вам время и формат проведения интервью.

3. Какой из методов выявления требований является самым информативным?
   - Интервью.
   - Опросный лист.
   - Изучение документации.
   - Самого информативного метода нет, каждый метод используется исходя из возможностей получения информации и поставленных задач.

4. В каких случаях выявление требований на основе изучения документации является затруднительным либо его использование нецелесообразно? (выберите несколько вариантов ответа)
   - в организации имеется только базовая документация.
   - в организации полностью отсутствует базовая документация.
   - в организации не поддерживается актуальность документации.
   - заказчик может предоставить часть информации только в обезличенном виде, т.е. без конкретных данных, например, шапки таблиц, шаблоны документов.
   - требуется быстрое получение информации.

5. Определите, что целесообразно предпринять следующей ситуации. Вы должны взять интервью у руководителя подразделения, но он под различными предлогами избегает встречи. У вас есть основания полагать, что он недостаточно компетентен и страшится показать свою неосведомленность по существу рассматриваемых вопросов. (выберите несколько вариантов ответа)
   - обратиться к вышестоящему руководителю с просьбой об оказании содействия в проведении интервью.
   - предложить руководителю подразделения заполнить опросный лист и использовать его для определения требований.
   - запросить у руководителя подразделения документацию и использовать ее для определения требований.
   - предложить руководителю подразделения назначить сотрудника для проведения интервью (при условии, что сотрудник обладает всей полнотой необходимой информации).

6. Определите приоритетный метод выявления требований, когда владельцем информации является руководитель управленческого подразделения (например, отдела ИБ).
   - Интервью.
   - Опросный лист.
   - Изучение документации.

7. Определите приоритетный метод выявления требований для следующей ситуации. Очень крупная организация, имеет сложную иерархическую и территориально распределенную структуру. Данных о наличии регламентирующей документации и степени ее актуальности нет.
   - Интервью.
   - Опросный лист.
   - Изучение документации.

8. При проведении интервью использование диктофона…
   - недопустимо.
   - является обязательным.
   - обязательно требует получения письменного согласия, интервьюируемого и руководства организации.
   - необходимо предварительно согласовать с интервьюируемым, факт подтверждения согласия должен быт записан на диктофон в начале интервью.

9. Выберите правильные утверждения, касающиеся использования технологии лингвистического анализа в InfoWatch Traffic Monitor (выберите несколько вариантов ответа):
   - детектирование опечаток по умолчанию включено и отключить его нельзя.
   - детектирование опечаток по умолчанию отключено, чтобы его включить нужно внести изменения в конфигурационный файл cas.conf.

- транслитерация по умолчанию включена и отключить ее нельзя.
- транслитерация по умолчанию отключена, чтобы ее включить нужно внести изменения в конфигурационный файл cas.conf.
- учет морфологии по умолчанию включен для всех терминов и отключить его нельзя.
- учет морфологии по умолчанию отключен для всех терминов чтобы его включить нужно внести изменения в конфигурационный файл cas.conf.
- учет морфологии настраивается для каждого термина.

10. Отметьте основные технологии, реализованные в InfoWatch Traffic Monitor (всегда включаются в поставку) (выберите несколько вариантов ответа):
    - Лингвистический анализ.
    - Текстовые объекты.
    - Эталонные документы.
    - Бланки.
    - Печати.
    - Выгрузки из баз данных.
    - Графические объекты.
    - Автолингвист.

Дисциплина «Правовые и организационные аспекты легитимизации DLP-системы»

1. На основание каких доводов работник может опротестовать свое увольнение в суде? (выберите несколько вариантов ответа)
    - Не установлен факт пересылки конфиденциальной информации.
    - Не со всеми регламентирующими документами, принятыми в компании, он был ознакомлен под подпись.
    - Сотрудник не знал, какая информация является конфиденциальной.
    - Его рабочей станцией мог воспользоваться другой сотрудник.
    - Работники не был осведомлен, что в компании ведется мониторинг и контроль.

2. В какой срок, компания должна получить объяснения от сотрудника, нарушившего политику информационной безопасности:
    - В этот же день.
    - В течение трех рабочих дней.
    - Не более двух дней.
    - При формирование необходимого пакета документов при судебном разбирательстве.

3. Относится ли InfoWatch Traffic Monitor к специальным техническим средствам, предназначенных для негласного получения информации?
    - Да, относится.
    - Нет, не относится.
    - Относятся только некоторые компоненты.
    - Да, согласно постановлению Правительства от 10.03.2000 N 214.

4. Какой документ необходимо утвердить в компании, где прописаны принципы и правила использование DLP-системы?
    - Приказ о защите информации.
    - Положение о защите информации ограниченного доступа.
    - Дополнительное соглашение к трудовому договору между работником и организацией.

- Регламент мониторинга и контроля.

5. Имеет ли право сотрудник использовать в личных целях информационные ресурсы компании, если это не оговорено в трудовом договоре?
   - Имеет.
   - Имеет, если это не запрещено другим актом.
   - Не имеет.
   - Имеет, после выполнения своих должностных обязанностей.

6. Какое взыскание может быть наложено на работника, при нарушении правил внутреннего трудового распорядка? (выберите несколько вариантов ответа)
   - Штраф
   - Увольнение
   - Выговор
   - Замечание
   - Депремирование

7. Необходима ли аттестация информационной системы и ввод её в действие?
   - Да, обязательно.
   - Нет, не обязательно.
   - По желанию руководства компании.
   - По требованию надзорных органов.

8. Какой приказ ФСТЭК утверждает требования о защите информации, не составляющей государственную тайну?
   - Приказ ФСТЭК № 53.
   - Приказ ФСТЭК № 21.
   - Приказ ФСТЭК № 17.
   - Приказ ФСТЭК № 12.

9. В чем заключаются обязательства сотрудника в целях охраны коммерческой тайны? (выберите несколько вариантов ответа)
   - Не разглашать информацию.
   - Не хранить информацию на внешнем носителе.
   - Не сообщать пароль от своего логина для входа на рабочую станцию.
   - Возместить причиненные убытки работодателю.

10. Могут ли операторы или иные лица, получившие персональные данные, передавать их третьим лицам?
    - Могут.
    - Не могут.
    - Могут с согласия субъекта персональных данных.
    - Могут по решению суда.

Дисциплина «Настройка и использование программных средств InfoWatch»

1. Какой режим создания запроса позволяет создать гибкую настройку параметров запроса?
   - Расширенный.
   - Обычный.

- Детальный.
- Пользовательский.

2. Какой раздел отчетности используются для оперативного получения статистических данных?
   - Сводка.
   - События.
   - Отчеты.
   - Выгрузки.

3. Как определяется время перехвата события?
   - Время перехвата события - это локальное время на агенте InfoWatch Device Monitor, где осуществляется перехват.
   - Время перехвата события - это локальное время на сервере InfoWatch Device Monitor.
   - Время перехвата события - это локальное время на сервере InfoWatch Traffic Monitor.
   - Время перехвата события - это глобальное время системе InfoWatch Traffic Monitor.

4. Какие фильтры доступны для поиска персон и компьютеров? (выберите несколько вариантов ответа)
   - Фильтр наличия снимков экрана.
   - Фильтр выбора персон и компьютеров с определенным статусом.
   - Поле поиска.
   - Фильтр даты создания карточки персоны или компьютера.

5. Какая группа политик отрабатывает непосредственно на агенте InfoWatch Device Monitor?
   - Политика защиты данных.
   - Политика защиты данных на агенте.
   - Политика контроля персон.
   - Политика хранения.

6. Каким образом можно запретить запуск определенного программного обеспечения для пользователя? (выберите несколько вариантов ответа)
   - Создать список Приложений.
   - Создать правило Application Monitor.
   - Назначить политику, содержащую правило запрета на группу сотрудников.
   - Назначить политику, содержащую правило запрета на группу компьютеров.
   - Создать Белый список.
   - Создать правило Device Monitor.
   - Создать правило File Monitor.

7. В каком разделе консоли управления InfoWatch Device Monitor можно управлять списками устройств, доступ к которым безусловно разрешен?
   - Белые списки.
   - Приложения.
   - Политики.
   - Группы компьютеров.

8. Каким образом можно назначить созданную политику? (выберите несколько вариантов ответа)
   - Созданную политику можно назначить через редактирование группы сотрудников.
   - Созданную политику можно назначить через редактирование группы компьютеров.

- Назначить, на кого будет действовать созданная политика, можно в разделе Политики.
- Назначить, на кого будет действовать созданная политика, можно в разделе Задачи.

9. Где можно собрать диагностическую информацию по работе агента InfoWatch Device Monitor удаленно?
   - В разделе Группы компьютеров.
   - В разделе Группы сотрудников.
   - Диагностическую информацию по работе агента можно собрать только локально на рабочей станции, где установлен агент.
   - Диагностическую информацию по работе агента можно собрать в логе приложении Microsoft Windows.

10. Какие приложения отображаются в протоколе приложений? (выберите несколько вариантов ответа)
   - все приложения, установленные на рабочих станциях.
   - все приложения, которые запускались на рабочих станциях.
   - все приложения, которые запускались на рабочих станциях, кроме критичных для работы компьютера.
   - все приложения, которые запускались на рабочих станциях кроме указанных в перечне «Исключение приложений из перехвата».
   - все приложения, которые запускались на рабочих станциях, кроме критичных для работы компьютера и указанных в перечне «Исключение приложений из перехвата».

Дисциплина «Внедрение и техническая поддержка Центра расследований InfoWatch»

1. Начиная с какой версии InfoWatch Traffic Monitor данные могут быть использованы в InfoWatch Prediction?
   - 7.0.
   - 7.2.
   - 6.11.
   - 7.8.

2. Могут ли одновременно быть установлены Infowatch Data Discovery и Infowatch Activity Monitor на одном сервере?
   - Да.
   - Нет.
   - Да, но не более двух продуктов на одном сервере.

3. Как получить токен Платформы для подключения Infowatch Device Monitor к Центру расследований InfoWatch?
   - скопировать через web-консоль Центра расследований InfoWatch.
   - запросить в технической поддержке InfoWatch.
   - запросить у аккаунт-менеджера InfoWatch.
   - скопировать с компьютера где установлен Центр Расследований InfoWatch.

4. Работа с какими системами управления базами данных (СУБД) поддерживается сервером InfoWatch Device Monitor? (выберите несколько вариантов ответа)

- Oracle Database 19.
- Microsoft SQL Server 2005, 2008, 2012, 2014, 2016, 2017, 2019 (Standard, Enterprise).
- PostgreSQL версии 13 и выше.
- DB2 Universal Database 7.2 и выше.
- MySQL 8.0 и выше.

5. Каким образом можно выбрать компьютер/компьютеры для установки агента InfoWatch Device Monitor? (выберите несколько вариантов ответа)
   - указать компьютер или группу компьютеров в соответствующем домене.
   - указать ip адрес компьютера.
   - импортировать данные с ip адресами компьютеров из соответствующего файла.
   - выполнить поиск компьютера по названию.
   - указать MAC адрес компьютера.
   - импортировать данные с MAC адресами компьютеров из соответствующего файла.

6. Определите порядок изменения статуса установки агента InfoWatch Device Monitor.
   - Подготовка.
   - В процессе.
   - Ожидание перезагрузки.
   - Выполнено.

7. Ключ шифрования (ключ защищенного канала) InfoWatch Device Monitor необходим для… (выберите несколько вариантов ответа)
   - обнаружения сервером агентов, ранее установленных на рабочих станциях.
   - шифрования данных, которые передаются с сервера InfoWatch Device Monitor на сервер InfoWatch Traffic Monitor.
   - шифрования данных, которые передаются с сервера InfoWatch Traffic Monitor на сервер InfoWatch Device Monitor.
   - шифрования данных, которые передаются между агентом InfoWatch Device Monitor и сервером InfoWatch Device Monitor.
   - обнаружения агентами всех доступных серверов в своем окружении.
   - шифровании данных, которые передаются между сервером InfoWatch Device Monitor и базой данных.

8. За какой минимальный период необходимы данные из Infowatch Traffic Monitor (с импортированной конфигурацией) для корректного расчета рейтинга по группам риска «Подготовка к увольнению» и «Нелояльные сотрудники» InfoWatch Prediction?
   - одна неделя.
   - две недели.
   - один месяц.
   - два месяца.

9. Каким образом решаются конфликты kubernetes и firewalld?
   - Для корректной работы kubernetes требуется отключить firewalld или настроить правила POD сети.
   - Для того чтобы избежать конфликтов, необходимо установить дополнительные пакеты.
   - Можно отключить kubernetes.

10. Как проверить статус работы установленных компонентов Платформы?
    - kubectl get pods -n infowatch.
    - iwtm status.
    - docker check status -n infowatch.

11. Какие пакеты необходимо установить для корректной работы платформы на сервере Oracle 7.9? (выберите несколько вариантов ответа)
    - socat.
    - conntrack-tools.
    - ocular.
    - kf5.

12. Где из перечисленных вариантов можно скачать пакет conntrack-tools, необходимый для работы платформы на Astra Linux 1.7? (выберите несколько вариантов ответа)
    - Из репозиториев Astra Linux.
    - Скачать по ссылке через wget.
    - Скопировать из другой системы, подключаемых устройств и т.д.

13. Что будет, если истечет срок действия Лицензии одного из продуктов Центра Расследования InfoWatch?
    - Функционал продукта, на который была выдана Лицензия будет недоступен.
    - Функционал всего Центра Расследований InfoWatch будет недоступен.
    - В Центр Расследований InfoWatch не будут поступать события от систем, с которыми была проведена синхронизация.

14. Для чего рекомендуется установить правила формирования паролей учетных записей и сроки их действия?
    - Для того, чтобы предотвратить несанкционированный вход в Систему и максимально обезопасить пользователя от компрометации его учетных данных третьими лицами.
    - Для того, чтобы пользователям было сложнее войти в систему.
    - Таковы правила Информационной Безопасности.

15. С какими системами можно настроить синхронизацию для получения информации о пользователях и связанных с ними данных? (выберите несколько вариантов ответа)
    - Microsoft Active Directory.
    - InfoWatch Traffic Monitor.
    - EWS - почтовым сервером.
    - СКУД.

16. Что означает серый цветовой индикатор справа от имени персоны в Досье?
    - Активный сотрудник.
    - Персоны, добавленные вручную.
    - Сотрудник с отключенной учетной записью в Microsoft Active Directory, либо имеющего неопределенный статус.
    - Персоны у которых истек срок действия учётной записи, но статус остался активным.

17. Правильно соотнесите продукты Центра Расследования InfoWatch и их описания:
    Продукты:
    - InfoWatch Vision.
    - InfoWatch Activity Monitor.
    - InfoWatch Prediction.
    - InfoWatch Data Discovery.

    Описания:
    - программное обеспечение, предназначенное для визуализации расследования инцидентов на основе данных, полученных от InfoWatch Traffic Monitor.
    - программное обеспечение, предназначенное для контроля деятельности сотрудников.
    - программное обеспечение, являющиеся инструментом предиктивной и поведенческой аналитики.
    - программное обеспечение, предназначенное для поиска конфиденциальной информации на общих сетевых ресурсах, рабочих станциях, серверах и в хранилищах документов.

18. Какое максимальное количество тегов можно добавить одному правилу маркировки событий?
    - 30.
    - 15.
    - 20.

19. Что такое Центр Расследований InfoWatch?
    - Центр расследований InfoWatch представляет собой платформу на которой могут быть развернуты четыре продукта InfoWatch
    - Центр расследований InfoWatch представляет собой отдельный продукт InfoWatch для проведения расследований
    - Центр расследований представляет собой платформу на которой могут быть развернуты все продукты InfoWatch

20. Для чего необходим раздел Главная?
    - Для для получения актуальной информации о нарушениях с помощью дашбордов.
    - Для накапливания собранной из разных источников информации и обобщения в расследования для последующего принятия решений или формирования отчетов.
    - Для получения наглядной статистики в виде таблиц, диаграмм и графиков, построенных по заданным условиям Единого фильтра и событиям, полученным из InfoWatch Traffic Monitor.

21. Можно ли удалить предустановленного пользователя Системы - Главный офицер безопасности?
    - Нет, удалить нельзя, но можно отредактировать.
    - Нет, нельзя ни удалить, ни отредактировать.
    - Да, конечно, наравне с добавленными пользователя.

22. Можно ли в разделе Главная создавать свои собственные дашборды?

- Да, можно создать свой уникальный дашборд и добавить на него виджеты из разных продуктов.
- Нет, можно использовать только предустановленные дашборды.
- Да, можно создать свой дашборд и добавить на него только общие виджеты для всех продуктов.

23. Каким образом мы можем сохранять информацию из виджетов средствами веб-консоли платформы? (выберите несколько вариантов ответа)
    - Выгружать содержимое виджетов в отчёт.
    - Сохранять в виде изображения.
    - Перенести информацию в раздел мониторинг и сохранить в pdf-формате.

24. Зачем нужен виджет "Действия с файлами? (выберите несколько вариантов ответа)
    - Позволяет увидеть массовые операции создания, перемещения или удаления файлов.
    - Позволяет выявить, какие сотрудники находятся в топе по действиям с файлами.
    - Позволяет копировать, перемещать или удалять файлы.

25. Что означает цвет внизу шкалы времени на Таймлайне?
    - Типы активности персоны в течении суток.
    - Работу в определенном приложении.
    - Зеленая полоса означает работу с видео файлами и сайтами, красная - работу с текстовыми данными, серая всю остальную активность.

26. Во вкладке "Наблюдение" мы можем подключиться к рабочей станции пользователя. Какие функции у нас присутствуют? (выберите несколько вариантов ответа)
    - Прослушать окружение.
    - Увидеть в реальном времени, что делает пользователь на рабочем столе.
    - Записать аудио дорожку.
    - Вывести текстовое уведомление на экран пользователя.

27. Что позволяет сделать синий значок "Play" на Таймлайне?
    - Прослушать аудиозапись, перейдя во вкладку "Аудиозаписи".
    - Просмотреть записанное видео с рабочего стола.
    - Получить название видеофайлов или сайтов, на которые заходил пользователь.
    - Всё вышеперечисленное.

28. Какое количество сканеров мы можем использовать при создании задачи сканирования?
    - 1.
    - 2.
    - 4.
    - 8.
    - То количество, которое мы сами зададим в настройках.

29. Можно ли при создании задачи сканирования добавлять собственные маски файлов?
    - Можно использовать только заранее созданные маски файлов.
    - Можно добавлять свои маски файлов.

30. Что произойдет, если при создании задачи удалить все предустановленные форматы файлов для сканирования?

- Система не сможет создать такую задачу, так как требуется выбрать хотя бы один из форматов файлов для сканирования.
- Система будет сканировать все файлы, находящиеся в выбранной директории.
- Задача будет создана, но такую задачу будет невозможно запустить.

31. Каким образом мы можем добавлять новые ресурсы в InfoWatch Device Monitor? (выберите несколько вариантов ответа)

- При помощи скрипта.
- Добавлять по одному вручную.
- Загрузить из текстового документа.

32. Для чего необходим раздел События?

- Для работы с событиями, загруженными из системы InfoWatch Traffic Monitor.
- Для проведения расследований инцидентов.
- Для просмотра статистики нарушений и активности пользователей.

33. Влияют ли настройки роли пользователя на отображение столбцов таблицы с событиями в разделе События?

- Да, столбцы таблицы с событиями отображаются с учетом настроек роли, выданной пользователю.
- Нет, для любого пользователя Системы отображаются все столбцы, вне зависимости от роли, выданной пользователю.
- Только предустановленный пользователь Офицер безопасности имеет возможность просматривать все столбцы таблицы с событиями, остальные пользователи Системы имеют возможность просматривать информацию из столбцов *Дата, Тип события, Отправитель, Получатель*.

34. Какая информация содержится на вкладке "Статистика нарушений" раздела Аналитика?

- На вкладке "Статистика нарушений" раздела Аналитика содержаться виджеты системы InfoWatch Vision, которые содержат статистическую информацию о нарушениях/нарушителях.
- На вкладке "Статистика нарушений" раздела Аналитика содержаться виджеты системы InfoWatch Activity Monitor, которые содержат статистическую информацию о нарушениях/нарушителях.
- На вкладке "Статистика нарушений" раздела Аналитика содержаться виджеты системы InfoWatch Prediction, которые содержат статистическую информацию о нарушениях/нарушителях.

35. Для чего необходим раздел Аналитика?

- Для возможности ознакомиться со статистикой в виде таблиц, диаграмм и графиков, построенных по заданным условиям Фильтра, и, событиям, полученным из InfoWatch Traffic Monitor.
- Для наблюдения за персонами онлайн.
- Для работы с файлами всех отчетов, созданных в Центре расследований InfoWatch.

36. Какие материалы можно добавить в расследование? (выберите несколько вариантов ответа)

- досье персон, подозреваемых в нарушении.

- Файлы.
- изображения.
- ссылки на web-ресурсы.
- статусы подозреваемых в нарушении.

37. В каком формате можно выгрузить и сохранить материалы расследования?

- документ .pdf
- документ .docx
- таблица .xlsx
- презентация .pptx

38. Какие действия доступны для расследования, помещенного в архив? (выберите несколько вариантов ответа)

- изменить имя.
- распечатать.
- удалить.
- обновить информацию.
- разархивировать.

39. В каком формате могут быть выгружены отчеты? (выберите несколько вариантов ответа)

- данные из виджетов в табличном представлении.
- растровый графический файл с расширением .png (для Графа связей).
- отчет с графиками и таблицами для печати (для Статистики активности).
- растровый графический файл с расширением .bmp (для Графа связей).
- данные из виджетов в виде документа с расширением .pdf.
- данные из виджетов в виде презентации с расширением .pptx.

40. Укажите последовательность разделов в имени ссылки выгруженного отчета:

- дата.
- время.
- название отчета.

41. Скачивание выбранного отчета выполняется...

- в папку "Загрузки".
- на Рабочий стол.
- в папку, заданную пользователем.
- в облачное хранилище.

42. Толщина ребра на графе связи зависит от...

- количества событий в связи: чем больше событий, тем толще линия связи.
- объема информации в событиях связи: чем больше объем информации, тем толще линия связи.
- количества нарушений в событиях связи: чем больше нарушений, тем толще линия связи.

43. Какие опции предлагаются для настройки цвета узла на графе связей? (выберите несколько вариантов ответа)

- Уровень нарушения.
- Должность.
- Отдел.
- Статус.
- Политика.
- Объект защиты.

44. На каком виджете в легенде указаны группы риска, которые учитываются при расчете?

- Рейтинг.
- Аномальный вывод информации.
- Подготовка к увольнению.
- Нетипичные внешние коммуникации.
- Отклонение от бизнес-процессов.
- Нелояльные сотрудники.

45. Какие паттерны включает в себя группа риска "Нетипичные внешние коммуникации"? (выберите несколько вариантов ответа)

- Переписка тет-а-тет.
- Новый для компании адресат.
- Новый для сотрудника адресат.
- Использование почты на телефоне.
- Отправка самому себе.

46. Перечислите допустимые методы сохранения событий в журнале безопасности (Выберите несколько вариантов ответа):
    - Затирать старые события по дням.
    - Затирать старые события по необходимости.
    - Не затирать события (чистка журнала вручную).
    - Затирать старые события по месяцам.
    - Затирать старые события по неделям.

47. Какая команда запускает обновление групповых политик?
    - gpupdate /force.
    - grpplcupd /force.
    - gpu /force.

48. Как расшифровывается аббревиатура NTLM?
    - NT LAN Manager.
    - Network Transferrable Local Machine.
    - NT Local Management.

49. С помощью какой команды возможно добавить учетную запись в дескриптор безопасности по умолчанию?
    - winrm quickconfig.
    - *Enable-PSRemoting –Force.*
    - winrm configSDDL default.

- winrm quickconfig –transport.

50. Возможно ли настроить подключение к нескольким контроллерам доменов одновременно?
    - Да, IW DAT поддерживает множественные подключения к различным контроллерам.
    - Нет, IW DAT подключается к единственному контроллеру.
    - Зависит от глобальных настроек Центра Расследований InfoWatch.
    - Зависит от типа лицензии.

51. Какое максимальное значение периода автоматической синхронизации?
    - 10080 минут.
    - 600 минут.
    - Не ограничено.

52. Перечислите типы данных, загружаемых при синхронизации (Выберите несколько вариантов ответа):
    - Пользователи.
    - События аудита.
    - Компьютеры.
    - Каталог Microsoft Active Directory.
    - Сервисные аккаунты.
    - Доступ к почте Microsoft Exchange.

53. Выберите правильную последовательность подключения почтового сервера:
    - Аудит инфраструктуры\Служба каталогов\Адрес контроллера\Адрес почтового сервера.
    - Настройки\Аудит инфраструктуры\Почтовый сервис\Адрес контроллера\Адрес почтового сервера\Логин и Пароль.
    - Аудит инфраструктуры\Почтовый сервис\Адрес контроллера\Адрес почтового сервера.

54. Расположите соответствующие определения согласно терминам:
    - **Аудит службы каталогов -** автоматизированные отчеты по уязвимым учетным записям, а также по событиям службы каталогов, связанным с риском несанкционированного доступа.
    - **Контроль изменения групп -** отслеживание действий с группами службы каталогов.
    - **Почтовые ящики -** мониторинг доступа к почтовым ящикам.

55. При создании нового пользователя в событиях аудита создается отдельное событие об изменении пароля. Свидетельствует ли такое событие о подозрительной активности?
    - Нет, не свидетельствует.
    - Да, свидетельствует.
    - Зависит от настроек Microsoft Active Directory.

56. Использует ли InfoWatch Data Access Tracker события из InfoWatch Traffic Monitor в своей работе?
    - Использует.
    - Не использует.
    - Зависит от типа установки продукта.

57. В каких разделах доступен Единый фильтр для InfoWatch Data Access Tracker? (Выберите несколько вариантов ответа)
    - Аналитика (Статистика нарушений).
    - События.
    - Персоны.

- Мониторинг.
- Риски.
- Хранение файлов.
- Расследования.

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

1. Дисциплина «Подготовка и реализация Концепции Политики защиты данных»

1. Разработать Политику защиты данных для предложенной ситуации (кейса) согласно соответствующему шаблону.
2. Реализовать разработанную Политику защиты данных в системах InfoWatch Traffic Monitor и InfoWatch Device Monitor.
3. Оценить результаты работы реализованной Политики защиты данных, при необходимости выполнить доработку Политики.

Шаблон Политики защиты данных

1. Используемые технологии анализа.

Перечислить технологии анализа, которые необходимо использовать для предотвращения утечки защищаемых данных

2. Объекты защиты (ОЗ)

№ п/п	Название ОЗ	Состав ОЗ

3. Списки отправителей/получателей

№ п/п	Название периметра	Список

4. Политики защиты данных

№ п/п	Название Политики	Тип политики	Объекты защиты	Правила срабатывания

5. Правила InfoWatch Device Monitor

перечислить правила, которые должны быть созданы в системе InfoWatch Device Monitor

Описание ситуаций (кейсов)

Кейс № 1

В последние полгода Агентство недвижимости «Удача» начало активно терять клиентов. Также некоторые девелоперы, представляющие квартиры в новостройках стали отказываться от сотрудничества и отзывать сделанные предложения.

Проведенное расследование показало, что за указанный период в Агентство начали активно приходить менеджеры по продажам-стажеры, которые после получения доступа к данным скачивали

нужную информацию и внезапно увольнялись. Опрос ушедших клиентов показал, что они получили более выгодные предложения от конкурирующего Агентства недвижимости «Мечта».

Для того, чтобы предотвратить подобные инциденты в будущем, была куплена DLP-система и приглашен аналитик для ее настройки под требования заказчика.

Необходимо обеспечить контроль:

- передачи на внешние почтовые адреса данных, касающихся объектов недвижимости: информация о стоимости квартир, основные параметры квартир (адрес, этаж, площадь, количество комнат, состояние), сведения об инфраструктуре (расположение парковок, детских садов, больниц, школ) и так далее
- передачи или копирования планов квартир

Необходимо исключить:

- передачу, копирование или печать информации из базы клиентов
- возможность снятия скриншотов при работе с базой клиентов

При этом следует вести особый контроль для новых сотрудников и обеспечить оперативное информирование офицера безопасности об инцидентах с их участием.

Кейс № 2

Совсем недавно у компании ООО «Товары.ру» начались проблемы с поставщиками, некоторые из них решили отказаться от сотрудничества по причине низкой закупочной цены. Также с недавнего времени один из главных конкурентов - ООО «Ценопад» начал открывать свои новые магазины через неделю после открытия точек ООО «Товары.ру», но в более удобных для потребителей местах (например, ближе к метро).

Служба информационной безопасности провела расследование, в результате которого стало ясно, что злоумышленником является бывший сотрудник компании, который теперь работает в компании конкурентов ООО «Ценопад». Служба ИБ предполагает, что при увольнении он смог забрать с собой части баз данных, которые содержали информацию о поставщиках и входящих закупочных ценах. Для того чтобы предотвратить подобные инциденты в будущем, была куплена DLP-система и приглашен аналитик для ее настройки под требования заказчика.

У бывшего сотрудника осталось несколько хороших знакомых в компании ООО «Товары.ру», которые могли передать информацию об открытии магазинов, персональных данных квалифицированных сотрудников и потенциально продолжают помогать ему. Сотрудникам службы безопасности известен круг общения бывшего сотрудника, и им хотелось бы предотвратить дальнейшие возможные утечки информации. ООО «Ценопад» не единственный конкурент на рынке, поэтому сотрудники службы ИБ высказали пожелание контролировать любые контакты и с другими конкурирующими торговыми сетями.

Кейс № 3

Одна из сотрудниц банка «SuperCredit» отправила около 20 кредитных историй клиенту банка вместо бюро. С ее стороны это были непреднамеренные действия. Девушка ошиблась, нажав ответить в сообщении клиента, вместо того чтобы ответить на сообщение-запрос из бюро. Таким образом, клиент получил не только свою кредитную историю, но и персональные данные (ФИО, серия и номер паспорта, ИНН, страховой номер ПФР) других клиентов банка. Данные клиентов оказались скомпрометированы в результате неумышленной утечки.

Сотрудница сразу же обратилась в службу ИБ, объяснив ситуацию. Данная ситуация произошла в банке впервые. Для того чтобы предотвратить подобные инциденты в будущем, была куплена DLP-система и приглашен аналитик для ее настройки под требования заказчика.

Начальник ИБ считает, что необходимо контролировать отдел кредитования на предмет массовой передачи персональных данных на внешние адреса (за исключением бюро) и копирование на внешние устройства. В случае попыток массовой передачи или копирования должна происходить блокировка.

Кейс № 4

Несколько дней назад в СМИ появилась информация о том, что нефтяная компания ООО «Нефтедобыча» готовится к заключению контракта с партнером АО «НПЗ». Сумма сделки, чертежи с трассами нефтепроводов и карты месторождений нефти попали в открытый доступ. В результате преждевременного раскрытия информации, партнер отказался от заключения контракта. В результате инцидента ООО «Нефтедобыча» понесла финансовые потери, а также была признана ненадежным партнером.

Служба информационной безопасности провела расследование, в результате которого стало ясно, что злоумышленник находится внутри компании. Для того чтобы предотвратить подобные инциденты в будущем, была куплена DLP-система и приглашен аналитик для ее настройки под требования заказчика.

Начальник ИБ имеет четкое понимание о том, что потенциальные нарушители могут быть среди отдела инженерного проектирования, управления технологий инжиниринга и бурения и оперативно-аналитического отдела. Имеются на руках примеры документации, чертежей, карт, которые были переданы в открытый доступ. Подобная информация в рамках рабочих процессов может передаваться только сотрудникам организаций ООО «Нефтьстрой», ПАО «Нефтепром».

Начальник настроен очень серьезно и планирует блокировать все потенциальные утечки информации.

ВОПРОСЫ И ЗАДАНИЯ К ЗАЧЕТУ

Теоретические вопросы

1. Назначение и принципы работы системы InfoWatch Traffic Monitor и комплементарных продуктов: InfoWatch Device Monitor, InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Prediction, InfoWatch Activity Monitor, InfoWatch Data Access Tracker, InfoWatch Device Control.
2. Аппаратные и программные требования к системе InfoWatch Traffic Monitor и его комплементарным продуктам: InfoWatch Device Monitor, InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Prediction, InfoWatch Activity Monitor, InfoWatch Data Access Tracker, InfoWatch Device Control.
3. Назначение и принципы работы основных служб InfoWatch Traffic Monitor.
4. Назначение ежедневных табличных пространств и параметры их настройки.
5. Режимы хранения данных InfoWatch Traffic Monitor.
6. Способы установки агента InfoWatch Device Monitor на рабочую станцию.
7. Принцип работы и порядок переключения режимов "черного" и "белого" списка приложений InfoWatch Device Monitor.
8. Назначение и принципы работы белого списка устройств InfoWatch Device Monitor.
9. Возможности перехвата информации системой InfoWatch Traffic Monitor (с каких устройств, по каким протоколам).
10. Способы формирования списка приложений InfoWatch Device Monitor.
11. Методы сбора требований: перечень, возможности, особенности использования.
12. Метод сбора требований – интервью, возможности и ограничения метода, способы повышения эффективности использования.
13. Метод сбора требований – опросный лист, возможности и ограничения метода, способы повышения эффективности использования.
14. Метод сбора требований – изучение документации, возможности и ограничения метода, способы повышения эффективности использования.
15. Организация процесса сбора требований.
16. Технология «Лингвистический анализ»: назначение, возможности, принципы работы.
17. Технология «Текстовые объекты»: назначение, возможности, принципы работы.
18. Технология «Эталонные документы»: назначение, возможности, принципы работы.
19. Технология «Бланки»: назначение, возможности, принципы работы.
20. Технология «Печати»: назначение, возможности, принципы работы.
21. Технология «Выгрузки из баз данных»: назначение, возможности, принципы работы.
22. Технология «Графические объекты»: назначение, возможности, принципы работы.

23. Технология «Автолингвист»: назначение, возможности, принципы работы.
24. Порядок подготовки данных для формирования Политики защиты данных
25. Содержание и элементы Политики защиты данных.
26. Федеральное законодательство РФ в сфере защиты информации.
27. Ответственность сотрудников за утечку данных.
28. Порядок привлечения к ответственности сотрудников, виновных в утечке данных.
29. Организационное обеспечение использования системы защиты от утечки данных.
30. Нормативно-правовое обеспечение использования системы защиты от утечки данных.

Практические задания

Практические задания по системе InfoWatch Traffic Monitor

1. Создать объект защиты, который обнаруживается в системе в случае нахождения категории «Финансы» и текстового объекта «ИНН» от 3-х вхождений.
2. Создать объект защиты, который обнаруживается в системе в случае обнаружения категории «Информация по счетам» или текстового объекта «БИК» или эталонного бланка «Выписка по счету» (от 5-ти заполненных полей).
3. Настроить политику с высоким уровнем нарушения при копировании на съемные устройства презентаций, отражающих информацию о стратегии компании.
4. Настроить политику со средним уровнем нарушения при обнаружении документов с грифами конфиденциальности на рабочих станциях сотрудников.
5. Настроить политику с высоким уровнем нарушения и тегом «На рассмотрение» при отправке по личной почте номеров кредитных карт в количестве от 5 штук.
6. Назначить на любых трех сотрудников статус «Под подозрением» и настроить на сотрудников с данным статусом политику контроля персон – отправка почтового уведомления офицеру безопасности при выполнении персоной действий с высоким уровнем нарушения.
7. Настроить политику контроля использования буфера обмена для сотрудников, имеющих статус «Под подозрением» и присвоения высокого уровня нарушения соответствующим событиям.
8. Добавить в карточку любой персоны еще один рабочий контакт.
9. Создать группу «Отдел кадров», внести туда несколько персон. Настроить политику таким образом, чтобы при отправке любой информации на веб-ресурсы из списка «Поиск работы» для любого сотрудника, кроме группы «Отдел кадров» формировалось событие с низким уровнем нарушения.
10. Создать периметр «Конкуренты», внести туда почтовые домены и адреса электронной почты. Настроить политику с высоким уровнем нарушения и уведомлением офицеру безопасности по почте при отправке финансовой информации в данный периметр.
11. Создать шаблон почтового уведомления, который будет отправляться нарушителю в случае блокировки передачи грифов конфиденциальности на файлообменники.
12. Создать тестового пользователя с возможностью просмотра Сводки, просмотра и выполнения отчетов, запросов. Также данный пользователь должен видеть события только со средним уровнем нарушения.
13. Найти события почты, в которых было передано не более 5 вложений.
14. Найти события отправки по почте, на которые сработали одновременно политики «Грифованная информация», «Управление компанией».
15. Найти все события, где в теме письма указано «Информация только для служебного пользования».
16. Сформировать любой запрос и сделать так, чтобы были видны только следующие поля (дата перехвата, id события, отправитель, получатель, уровень нарушения). Отсортировать события по id события в порядке убывания.
17. Выгрузить события с вложениями, которые являются результатом выполнения пункта 14.
18. Создать новую панель сводки, внести туда следующие виджеты: Статистика по политикам, Динамика нарушений, Топ нарушителей, Количество нарушений за период и выгрузить ее.

19. Сделать так, чтобы в виджете Статистика по политикам отображались следующие политики «Грифованная информация», «Финансовая информация». А виджете топ нарушителей была статистика только по тем сотрудникам, которые имеют статус «Под подозрением».
20. Построить отчет, содержащий информацию о сотрудниках, которые являются активными пользователями социальных сетей и выгрузить ее в формате xls(x).

Практические задания по системе InfoWatch Device Monitor

1. Создать политику теневого копирования для почтовых сообщений, передаваемых по всем каналам с помощью протоколов SMTP, IMAP и назначить ее на группу компьютеров.
2. Создать политику, разрешающую только скачивание файлов со следующих облачных хранилищ: YandexDisk, OneDrive, DropBox и назначить ее на группу сотрудников.
3. Создать политику снятия теневой копии файлов, копируемых на съемные носители и при этом исключить файлы .tmp и назначить ее на группу компьютеров.
4. Создать политику, запрещающую использование приложения «Блокнот» и назначить ее на группу сотрудников.
5. Настроить на группу сотрудников перехват вставки из буфера обмена в следующие приложения: Microsoft Word, Adobe Reader, Microsoft Excel.
6. Запретить использование Skype и настроить контроль сообщений, передаваемых через Telegram для группы сотрудников.
7. Предоставить полный доступ к съемным устройствам хранения группе сотрудников на один день.
8. Настроить политику снятия скриншотов в случае запуска таких приложений, как Skype, Paint для определенной группы сотрудников.
9. Запретить для определенной группы компьютеров запуск любых приложений, помимо Skype.
10. Установить для определенной группы компьютеров сокрытие отображения уведомлений сотруднику.

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Требования к квалификации педагогических кадров, представителей предприятий и организаций, обеспечивающих реализацию образовательного процесса

Требования к образованию и обучению лица, занимающего должность преподавателя: высшее образование - специалитет или магистратура, направленность (профиль) которого, как правило, соответствует преподаваемому учебному курсу, дисциплине (модулю).

Дополнительное профессиональное образование на базе высшего образования (специалитета или магистратуры) - профессиональная переподготовка, направленность (профиль) которой соответствует преподаваемому учебному курсу, дисциплине (модулю).

Педагогические работники обязаны проходить в установленном законодательством Российской Федерации порядке обучение и проверку знаний и навыков в области охраны труда.

Рекомендуется обучение по дополнительным профессиональным программам по профилю педагогической деятельности не реже чем один раз в три года.

Требования к опыту практической работы: при несоответствии направленности (профиля) образования преподаваемому учебному курсу, дисциплине (модулю) – наличие у преподавателей опыта работы в области профессиональной деятельности, осваиваемой обучающимися или соответствующей преподаваемому учебному курсу, дисциплине (модулю).

Преподаватель: стаж работы в образовательной организации не менее одного года; при наличии ученой степени (звания) - без предъявления требований к стажу работы.

Особые условия допуска к работе: отсутствие ограничений на занятие педагогической деятельностью, установленных законодательством Российской Федерации.

Прохождение обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также внеочередных медицинских осмотров (обследований) в порядке, установленном законодательством Российской Федерации

Прохождение в установленном законодательством Российской Федерации порядке аттестации на соответствие занимаемой должности.

Требования к материально-техническим условиям

Образовательный процесс осуществляется с применением дистанционных образовательных технологий, с учетом чего созданы условия для функционирования электронной информационно-образовательной среды.

Требования к оборудованию слушателя для проведения занятий

- персональный компьютер под управлением операционной системы Windows 10 и выше;
- видеокамера, микрофон и аудиосистема (колонки или наушники), подключенные к компьютеру;
- пакет Microsoft Office 2016 и выше;
- выход в Интернет;
- Интернет-браузер;
- возможность установки и использования приложения «Ассистент».

Требования к информационным и учебно-методическим условиям

Список литературы

1. InfoWatch Traffic Monitor. Руководство по установке. https://kb.infowatch.com/pages/viewpage.action?pageId=217786377
2. InfoWatch Traffic Monitor. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=217786851
3. InfoWatch Traffic Monitor. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=217787298
4. InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию. https://kb.infowatch.com/pages/viewpage.action?pageId=217778197
5. InfoWatch Device Monitor. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=217778288
6. InfoWatch Vision. Руководство по установке. https://kb.infowatch.com/pages/viewpage.action?pageId=224576566
7. InfoWatch Vision. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=224576598
8. InfoWatch Vision. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=224576851
9. InfoWatch Activity Monitor. Руководство по установке. https://kb.infowatch.com/pages/viewpage.action?pageId=224578028
10. InfoWatch Activity Monitor. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=224576598
11. InfoWatch Activity Monitor. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=224576851

12. InfoWatch Data Discovery. Руководство по установке. https://kb.infowatch.com/pages/viewpage.action?pageId=224579999
13. InfoWatch Data Discovery. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=224580036
14. InfoWatch Data Discovery. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=224580265
15. InfoWatch Prediction. Руководство по установке. https://kb.infowatch.com/pages/viewpage.action?pageId=224581001
16. InfoWatch Prediction. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=224581032
17. InfoWatch Prediction. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=224581246

Нормативные правовые акты

1. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ
2. «Конституция Российской Федерации» принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020
3. «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ
4. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ
5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ
6. Федеральный закон "О коммерческой тайне" от 29.07.2004 № 98-ФЗ
7. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ

Интернет-ресурсы

1. http://www.consultant.ru/
2. https://www.infowatch.ru/
3. https://habr.com/ru/all/
4. https://мойассистент.рф