ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«АКАДЕМИЯ ИНФОВОТЧ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 02214E9D008AB20DBB4227DE786E91AAFB
Владелец: ХАРИТОНОВ СЕРГЕЙ ВЛАДИМИРОВИЧ
Действителен: с 20.02.2025 до 20.05.2026

Утверждена

Генеральный директор
С.В. Харитонов

МП

Дополнительная профессиональная программа
повышения квалификации
«Углубленный курс по проведению расследований с помощью продуктов InfoWatch»

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 «Углубленный курс по проведению расследований с помощью продуктов InfoWatch».

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 защиты информации от утечек, анализа событий, коммуникаций сотрудников, активности пользователей и использования средств предиктивной аналитики
- практическая подготовка для выполнения работ по проведению расследований с использованием следующих продуктов InfoWatch: Activity Monitor, Data Discovery, Prediction, Vision.

Категория слушателей:

- инженер по защите информации
- специалист по защите информации I категории
- специалист по защите информации II категории
- специалист по защите информации

Организационно-педагогические условия

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

Срок обучения: 50/4/1 (ак. час, нед., мес.).

Режим занятий: 45 академических часов самостоятельного обучения с использованием дистанционных образовательных технологий, 5 академических часов итоговой аттестации (защита итоговой аттестационной работы) с использованием средств видео-конференц-связи.

Форма обучения: заочная с применением дистанционных образовательных технологий

Характеристика профессиональной деятельности слушателей

Область профессиональной деятельности слушателей:

- проведение расследований, связанных с обеспечением защиты данных от утечек

Специалист по защите данных от утечек готовится к следующим видам деятельности: к участию в проведении расследований, связанных с утечкой данных, 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 защиты итоговой аттестационной работы 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.

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), итоговая аттестационная работа для итоговой аттестации.

Методическими материалами к Программе является 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

УГЛУБЛЕННЫЙ КУРС ПО ПРОВЕДЕНИЮ РАССЛЕДОВАНИЙ С ПОМОЩЬЮ ПРОДУКТОВ INFOWATCH

(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	Использование и администрирование Центра расследований InfoWatch	27,0	8,2	17,3	1,5	Тестирование
2	Проведение расследований с помощью продуктов InfoWatch	18,0	4,5	13,0	0,5	Тестирование
3	ИТОГОВАЯ АТТЕСТАЦИЯ	5,0			5,0	Итоговая аттестационная работа
	Всего:	50,0	12,7	30,3	7,0	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
ПО ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЕ
повышения квалификации

УГЛУБЛЕННЫЙ КУРС ПО ПРОВЕДЕНИЮ РАССЛЕДОВАНИЙ С ПОМОЩЬЮ ПРОДУКТОВ INFOWATCH

(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	Использование и администрирование Центра	27,0	8,2	17,3	1,5	Тестирование

	расследований InfoWatch					
1.1	Центр расследований - единый интерфейс средств информационной безопасности Info Watch	1,5	0,5	1,0		
1.2	Общие функции Центра расследований	3,3	1,3	2,0		
1.3	InfoWatch Vision	2,7	0,7	2,0		
1.4	InfoWatch Activity Monitor	3,1	1,1	2,0		
1.5	InfoWatch Prediction	1,6	0,6	1,0		
1.6	InfoWatch Data Discovery	2,8	0,8	2,0		
1.7	InfoWatch Data Access Tracker	1,8	0,6	1,2		
1.8	InfoWatch Device Control	2,0	0,4	1,6		
1.9	Настройки Центра расследований	6,7	2,2	4,5		
	Тестирование	1,5			1,5	
2	**Проведение расследований с помощью продуктов InfoWatch**	**18,0**	**4,5**	**13,0**	**0,5**	**Тестирование**
2.1	Принципы проведения расследований с помощью продуктов InfoWatch	1,5	0,5	1,0		
2.2	Сценарий проведения расследования с использованием InfoWatch Data Discovery	1,6	0,6	1,0		
2.3	Сценарий проведения расследования с использованием InfoWatch Vision	2,2	0,7	1,5		

2.4	Сценарий проведения расследования с использованием InfoWatch Activity Monitor	2,8	0,8	2,0		
2.5	Сценарий проведения расследования с использованием InfoWatch Prediction	2,2	0,7	1,5		
2.6	Сценарий проведения комплексного расследования	3,2	1,2	2,0		
2.7	Практика проведения расследований с помощью продуктов InfoWatch			4,0		
	Тестирование	0,5			0,5	
3	**ИТОГОВАЯ АТТЕСТАЦИЯ**	**5,0**			**5,0**	**Итоговая аттестационная работа**
	Всего:	**50,0**	**12,7**	**30,3**	**7,0**	

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: 1,5-2,0 академических часа в день (кроме итоговой аттестации с использованием средств видео-конференц-связи). 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	Использование и администрирование Центра расследований InfoWatch	СР	1,5	2,0	1,5	2,0	1,5	2,0	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5													
2	Проведение расследований с помощью продуктов InfoWatch	СР																		1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	
3	Итоговая аттестация																															5,0

Рабочая программа учебной дисциплины «Использование и администрирование Центра расследований InfoWatch» (код В)

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

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 27,0 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 17,3 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	
1	**Использование и администрирование Центра расследований InfoWatch**	**27,0**	**8,2**	**17,3**	**1,5**	**Тестирование**
1.1	Центр расследований - единый интерфейс средств информационной безопасности Info Watch	1,5	0,5	1,0		
1.2	Общие функции Центра расследований	3,3	1,3	2,0		
1.3	InfoWatch Vision	2,7	0,7	2,0		
1.4	InfoWatch Activity Monitor	3,1	1,1	2,0		
1.5	InfoWatch Prediction	1,6	0,6	1,0		
1.6	InfoWatch Data Discovery	2,8	0,8	2,0		
1.7	InfoWatch Data Access Tracker	1,8	0,6	1,2		
1.8	InfoWatch Device Control	2,0	0,4	1,6		
1.9	Настройки Центра расследований	6,7	2,2	4,5		
	Тестирование	1,5			1,5	

Тема 1.1. 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 1.2. Общие функции Центра расследований

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

Тема 1.3. 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 1.4. 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 1.5. InfoWatch Prediction

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

Тема 1.6. 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 1.7 InfoWatch Data Access Tracker

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

Тема 1.8 InfoWatch Device Control

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

Тема 1.9. Настройки Центра расследований

- Настройки системы.
- Настройки продуктов.
- Настройка правил Device Monitor для Activity Monitor.

Рабочая программа учебной дисциплины «Проведение расследований с помощью продуктов InfoWatch» (код B)

Цель: обеспечение глубоких знаний обучающихся в области проведения расследований с использованием следующих продуктов InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Prediction, InfoWatch Activity 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 проведения расследований с помощью программных продуктов InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Activity Monitor, InfoWatch Prediction.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Принципы проведения расследований с помощью продуктов InfoWatch;
- Последовательность действий при проведении расследования с помощью продуктов InfoWatch;
- Возможности продуктов InfoWatch Vision, Activity Monitor, Prediction и Data Discovery для проведения расследований.

Уметь:

- Определять какой продукт/продуты нужно использовать в зависимости от цели и задач расследования;
- Определять сценарий проведения расследования с использованием одного или нескольких продуктов InfoWatch;
- Выполнять действия по анализу событий и активности сотрудника, фиксировать данные в Расследовании;
- Подводить итоги и формулировать рекомендации по результатам расследования.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 18,0 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 13,0 академических часов.

№ 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	**Проведение расследований с помощью продуктов InfoWatch**	**18,0**	**4,5**	**13,0**	**0,5**	**Тестирование**
2.1	Принципы проведения расследований с помощью продуктов InfoWatch	1,5	0,5	1,0		
2.2	Сценарий проведения расследования с использованием	1,6	0,6	1,0		

	InfoWatch Data Discovery					
2.3	Сценарий проведения расследования с использованием InfoWatch Vision	2,2	0,7	1,5		
2.4	Сценарий проведения расследования с использованием InfoWatch Activity Monitor	2,8	0,8	2,0		
2.5	Сценарий проведения расследования с использованием InfoWatch Prediction	2,2	0,7	1,5		
2.6	Сценарий проведения комплексного расследования	3,2	1,2	2,0		
2.7	Практика проведения расследований с помощью продуктов InfoWatch			4,0		
	Тестирование	0,5			0,5	

Тема 2.1. Принципы проведения расследований с помощью продуктов InfoWatch

- Порядок проведения расследования в зависимости от вводных данных
- Последовательность действий при проведении расследования

Тема 2.2. Сценарий проведения расследования с использованием InfoWatch Data Discovery

- Описание ситуации
- Алгоритм действий для проведения расследования с помощью InfoWatch Data Discovery
- Вводные данные
- Проведение расследования с помощью InfoWatch Data Discovery
- Итоги проведенного расследования
- Рекомендации по итогам расследования

Тема 2.3. Сценарий проведения расследования с использованием InfoWatch Vision

- Описание ситуации
- Алгоритм действий для проведения расследования с помощью InfoWatch Vision

- Вводные данные
- Проведение расследования с помощью InfoWatch Vision
- Итоги проведенного расследования
- Рекомендации по итогам расследования

Тема 2.4. Сценарий проведения расследования с использованием InfoWatch Activity Monitor

- Описание ситуации
- Алгоритм действий для проведения расследования с помощью InfoWatch Activity Monitor
- Вводные данные
- Проведение расследования с помощью InfoWatch Activity Monitor
- Итоги проведенного расследования
- Рекомендации по итогам расследования

Тема 2.5. Сценарий проведения расследования с использованием InfoWatch Prediction

- Описание ситуации
- Алгоритм действий для проведения расследования с помощью InfoWatch Prediction
- Вводные данные
- Проведение расследования с помощью InfoWatch Prediction
- Итоги проведенного расследования
- Рекомендации по итогам расследования

Тема 2.6. Сценарий проведения комплексного расследования

- Описание ситуации
- Алгоритм действий для проведения комплексного расследования
- Вводные данные
- Проведение комплексного расследования
- Итоги проведенного расследования
- Рекомендации по итогам расследования

Тема 2.7 Практика проведения расследований с помощью продуктов InfoWatch

- Анализ ситуации и вводных данных
- Определение разделов Центра расследований, необходимых для проведения расследования
- Выполнение расследования, фиксация результатов, итогов и рекомендаций.

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.

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 защиты итоговой аттестационной работы.

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

Лицам, освоившим образовательную программу повышения квалификации «Углубленный курс по проведению расследований с помощью продуктов InfoWatch» 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	**Специалист должен обладать профессиональными компетенциями (ПК), соответствующими основным видам профессиональной деятельности:** - Выполнение установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования	**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

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	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	• 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 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.

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 зачтено	Оценка **«Не зачтено»** выставляется слушателю, который не знает значительной части программного материала, допускает существенные ошибки. Менее 70% правильных ответов при решении тестов.

Оценка качества освоения учебной программы проводится в процессе итоговой аттестации в форме защиты итоговой аттестационной работы.

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 более 2-х ошибок в итоговой аттестационной работе.
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. Более 2-х ошибок в итоговой аттестационной работе.

Фонд оценочных средств

Оценочные материалы

ТЕСТОВЫЕ ВОПРОСЫ

Дисциплина «Использование и администрирование Центра расследований InfoWatch»

1. Что означает серый цветовой индикатор справа от имени персоны в Досье?

- Активный сотрудник
- Персоны, добавленные вручную
- Сотрудник с отключенной учетной записью в AD, либо имеющего неопределенный статус
- Персоны, у которых истек срок действия учётной записи, но статус остался активным

2. Правильно соотнесите продукты Центра Расследования 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

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

4. Что такое Центр Расследований?
   - Центр расследований представляет собой платформу на которой могут быть развернуты шесть продуктов InfoWatch
   - Центр расследований представляет собой отдельный продукт InfoWatch для проведения расследований
   - Центр расследований представляет собой платформу на которой могут быть развернуты все продукты InfoWatch

5. Для чего необходим раздел Главная?
   - 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 Traffic Monitor

6. 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

7. Можно ли в разделе Главная создавать свои собственные дашбоарды?
   - Да, можно создать свой уникальный дашборд и добавить на него виджеты из разных продуктов
   - Нет, можно использовать только предустановленные дашбоарды

- Да, можно создать свой дашборд и добавить на него только общие виджеты для всех продуктов

8. 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

9. 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

10. 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

11. 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

12. 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

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

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

15. 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

16. Каким образом мы можем добавлять новые ресурсы в Device Monitor? (Выберите несколько вариантов ответа)

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

17. 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

18. 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*.

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

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

20. 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 Traffic Monitor
- Для наблюдения за персонами онлайн
- Для работы с файлами всех отчетов, созданных в Центре расследований

21. Какие материалы можно добавить в расследование? (Выберите несколько вариантов ответа)

- досье подозреваемых в нарушении
- файлы
- изображения
- ссылки на web-ресурсы
- статусы подозреваемых в нарушении

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

- изменить имя
- распечатать

- удалить
- обновить информацию
- разархивировать

23. 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

24. Укажите последовательность разделов в имени ссылки выгруженного отчета
    - дата
    - время
    - название отчета

25. Скачивание выбранного отчета выполняется...
    - в папку "Загрузки"
    - на Рабочий стол
    - в папку, заданную пользователем
    - в облачное хранилище

26. 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

27. Какие опции предлагаются для настройки цвета узла на графе связей? (Выберите несколько вариантов ответа)
    - Уровень нарушения
    - Должность
    - Отдел
    - Статус
    - Политика
    - Объект защиты

28. На каком виджите 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

29. 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

30. Могут ли над расследованием работать (редактировать его) несколько офицеров безопасности одновременно?

- Да. Над расследованием могут работать (редактировать его) одновременно несколько офицеров безопасности, однако удалить расследование может только его автор или Главный офицер.
- Нет. Над одним расследованием одномоментно может работать только один офицер безопасности.
- Да. Над расследованием могут работать (редактировать его) одновременно несколько офицеров безопасности, удалить расследование может может любой офицер безопасности.

Дисциплина «Проведение расследований с помощью продуктов InfoWatch»

1. Укажите последовательность этапов проведения расследования.
   - Создать новое Расследование, добавить описание ситуации и известные факты, а также соответствующие файлы при их наличии.
   - Определить алгоритм действий для проведения расследования.
   - Провести анализ событий и действий пользователей с помощью соответствующих инструментов.
   - Подвести итоги и зафиксировать их в Расследовании.
   - Подготовить и предоставить рекомендации по итогам Расследования.

2. Как IW Data Discovery может осуществлять поиск дубликатов файлов? (Выберите несколько вариантов ответа)
   - по хэшу
   - по размеру
   - по содержанию
   - по расширению
   - по метаданным
   - по заголовку
   - по истории перемещения

3. В чем заключается основная задача IW Data Discovery?
   - собирать файлы в соответствии с заданиями и отправлять в IW Traffic Monitor для обработки, анализа и применения политик защиты данных
   - отслеживать операции чтения/записи, копирования и удаления файлов
   - блокировать передачу файлов за периметр организации в соответствии с настроенными политиками защиты данных
   - выявлять факты превышения прав доступа к файлам

4. Каким образом можно выгрузить скриншоты используя инструмент «Снимки экрана»?

- отдельный скриншот или несколько скриншотов выделенных вручную, которые выгружаются в архив с расширением .zip
- только отдельный скриншот, который выгружается в графический файл с расширением .jpg
- отдельный скриншот или несколько скриншотов за указанный период или дату, которые выгружаются в архив с расширением .zip
- отдельный скриншот или несколько скриншотов, связанных с активностью определенного типа, которые выгружаются в архив с расширением .zip

5. Каким образом можно обеспечить получение пароля от зашифрованного архива?
   - настроить политику перехвата ввода текста с клавиатуры и перехвата буфера обмена при работе с архиваторами
   - настроить политику создания скриншотов при работе с архиваторами
   - настроить политику контроля операций чтения/записи при работе с архиваторами
   - настроить включение записи экрана пользователя при работе с архиваторами

6. Как можно сформировать список событий, на основе которых определен рейтинг по группе риска для конкретной персоны?
   - в разделе «Риски» - «Рейтинг» установить фильтр по Группе риска, выбрать персону – в новом окне откроется вкладка с данными персоны по выбранной группе риска
   - в разделе «События» установить фильтр на определенную Группу риска, Персону и Дату – будут выведены соответствующие события
   - в разделе «Риски» - «Рейтинг» щелкнуть на легенду (справа от персоны) на виджите соответствующей группы риска для выбранной персоны - в новом окне откроется вкладка с данными персоны по выбранной группе риска
   - в разделе «Риски» - «Рейтинг» установить фильтр по Группе риска, Персоне и Дате, и сохранить отчет, список событий будет выгружен в формате .xlsx

7. Как можно посмотреть в IW Traffic Monitor детали событий, на основе которых определен рейтинг персоны по выбранной группе риска? (Выберите несколько вариантов ответа)
   - в разделе «Персоны» - «Группы риска» нажать кнопку «Просмотр событий» и перейти к событиям в IW Traffic Monitor
   - в разделе «Персоны» - «Группы риска» скопировать ID события, перейти в IW Traffic Monitor и найти событие по его ID
   - выбрать событие, добавленное в Расследование и дважды щелкнуть по нему левой кнопкой мыши – будет выполнен переход к событию IW Traffic Monitor
   - в разделе «События» установить фильтр на определенную Группу риска, Персону и Дату, нажать кнопку «Просмотр событий» и перейти к событиям в IW Traffic Monitor

8. Установите соответствие продукта и задачи, решаемой при проведении расследования.
   Продукты:
   - InfoWatch Vision
   - InfoWatch Activity Monitor
   - InfoWatch Prediction
   - InfoWatch Data Discovery

   Решаемые задачи:
   - Анализ статистики и Графа связей.
   - Анализ действий сотрудников.

- Анализ аномалий и выявление угроз в поведении сотрудников.
- Аудит хранения данных на рабочих станциях и серверах.

9. Где отображаются данные, собранные в Системе и визуализированные на экране в виде Графа связей?
    - на сайдбаре
    - на виджите «Граф связей»
    - на виджите «Аналитика по группам/персонам»
    - на виджите «Статистика»

10. Какой раздел Центра расследований можно использовать для анализа конкретных событий независимо от того, какие установлены продукты?
    - События
    - Аналитика
    - Мониторинг
    - Расследования
    - Отчеты

ИТОГОВАЯ АТТЕСТАЦИОННАЯ РАБОТА

1. Провести анализ ситуации, определить последовательность действий для проведения расследования с помощью продуктов InfoWatch.
2. Провести расследование с помощью продуктов InfoWatch, фиксируя в разделе «Расследования» его ход, итоги и рекомендации.

Описание ситуаций (кейсов)

Кейс № 1

Компания ООО «ИнфоСтрах» занимается страхованием имущества, здоровья и ответственности физических и юридических лиц.

Есть риск, что увольняющийся сотрудник может забрать с собой конфиденциальную информацию с целью получения какой-либо выгоды.

В связи с этим принято решение по введению мер анализа поведения сотрудников, для выявления специалистов, готовящихся к уходу. Особое внимание необходимо уделить отделу продаж, так как его сотрудники часто забирают клиентскую базу с собой. В случае выявления подобных специалистов, необходимо провести расследование. В рамках которого, определить, не собираются ли они предпринять незаконные действия по хищению конфиденциальной информации. Необходимо провести расследование с использованием продуктов IW для выявления потенциально опасной активности.

Вводные данные

- Сотрудникам запрещено хранить базу клиентов данных или ее части на рабочих станциях, обработка этих данных происходит на сервере. Данное прописано в «Политике обработке конфиденциально информации» принятой в организации.
- Сотрудникам запрещено использовать информацию, принадлежащую ООО «ИнфоСтрах», данные о клиентах и иные конфиденциальные сведения, ставшие известными в процессе выполнения трудовой деятельности, в личных целях. Это закреплено в «Политики безопасности организации» и законодательством РФ.
- Сотрудникам запрещено использовать вычислительные ресурсы и каналы связи компании в личных целях, ООО «ИнфоСтрах» не предоставляет услуг по предоставлению связи. Данный пункт закреплен в «Правилах внутреннего распорядка»
- В ТМ настроены Технологии и ОЗ для чувствительных данных внутри компании. Импортирована отраслевая БКФ «Страхование». В данном случае используются следующие политики защиты

данных:

- Страхование
- Персональные данные

Необходимые разделы для проведения расследования

- В IW DD: Хранение файлов → Информация о файлах
- В IW Vision: Аналитика → Граф Связей
- В IW AM: Мониторинг → Наблюдение
- Мониторинг → Снимки экрана
- Мониторинг → Действия с файлами
- В IW Prediction: Риски → Рейтинг

Дополнительно потребуется раздел «Персоны» для проверки легитимности доступа к файлам и «цифрового досье», и, раздел «События» для анализа конкретных событий.

Расследование удобно собирать и фиксировать в разделе «Расследования» (актуально для всех продуктов).

В данном сценарии расследование начинается **от сложившейся ситуации → до выявления подробностей** и **участников**.

Кейс № 2

Компания "Глобал Авто" является одним из лидеров рынка параллельного импорта автомобилей в России.

В последнее время руководитель отдела закупок компании заметил нетипичное поведение подчиненного менеджера Германа Мамонтова. Сотрудник стал себя вести более замкнуто, а при личном обращении к нему коллег, часто сразу блокировал рабочую станцию.

В связи с этим, руководство компании поручило Вам провести комплексное расследование в отношении Германа Мамонтова.

Вводные данные

- Сотрудникам организации запрещено передавать за периметр компании, копировать, хранить на локальной рабочей станции выгрузки из баз данных (файл формата csv) на своих рабочих местах;
- В компании установлена жесткая политика взаимодействия с главным конкурентом Rus-AutoImport.
- В силу п. 1,2 в системе IWTM Настроены политики:
  - посещение сайтов конкурента:
    - защищаемые данные: «Сайты конкурентов» → ОЗ: «Сайт конкурента» → Технологии → ТО «АвтоImport»
    - правило: Передачи информации. Срабатывает при посещении раздела «Контакты» на сайте конкурента rus-auto-import.ru/kontaktyi
- копирование контактов конкурента:
  - защищаемые данные: «Контакты конкурентов» → ОЗ: «Сайт конкурента» → Технологии ТО → «Ссылки на сайт конкурентов»
  - правила: Работа в приложениях → Буфер обмена. Детектирует копирование почтового адреса конкурента (info@rus-auto-import.ru) AutoImport из браузера chrome.exe
- критическая информация:

    - защищаемые данные: «БД Поставщика» (содержит выгрузку БД Автомобили от поставщика.csv) → ОЗ: БД Поставщика → Технологии: Выгрузки из БД → «БД поставщика» → Автомобили от поставщика.csv
    - правила:
        - Передачи за пределы периметра компании, используя электронную почту.
        - Копирование данных в облако\съемные устройства.
        - Хранение данных на рабочей станции сотрудника.
- В системе IWDM в «Политика теневого копирования» добавлены следующие правила:
    - «Посещение сайтов конкурентов» → Перехватчик Screenshot Monitor. Правило отслеживает посещение раздела «Контакты» на сайте rus-auto-import.ru/kontaktyi/
    - «Копирование из браузера» → перехватчик Clipboard Monitor. Отслеживает копирование из браузера chrome.exe.

В данном сценарии расследование начинается с выявления и анализа **нетипичного поведения сотрудника → до выявления подробностей.**

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 MS 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 администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=217786851
2. InfoWatch Traffic Monitor. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=217787298
3. InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию. https://kb.infowatch.com/pages/viewpage.action?pageId=217778197
4. InfoWatch Device Monitor. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=217778288
5. InfoWatch Vision. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=224576598
6. InfoWatch Vision. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=224576851
7. InfoWatch Activity Monitor. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=224576598
8. InfoWatch Activity Monitor. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=224576851
9. InfoWatch Data Discovery. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=224580036
10. InfoWatch Data Discovery. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=224580265
11. InfoWatch Prediction. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=224581032
12. InfoWatch Prediction. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=224581246
13. InfoWatch Data Access Tracker. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=24204886
14. InfoWatch Data Access Tracker. Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=242049121
15. InfoWatch Device Control. Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=242043440
16. InfoWatch Device Control. Руководство пользователя.

https://kb.infowatch.com/pages/viewpage.action?pageId=242043534

Интернет-ресурсы

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