**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**
**«Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы.»**

**Форма обучения: заочная**
**с применением дистанционных образовательных технологий**

**Москва 2025**

**Оглавление**

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА ..... 3
УЧЕБНЫЙ ПЛАН ..... 6
УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН ..... 7
КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК ..... 8
Рабочая программа учебной дисциплины «Обзор аналитических работ» (код В) ..... 9
Рабочая программа учебной дисциплины «Правовые и организационные аспекты легитимизации DLP системы» (код В) ..... 11
Рабочая программа учебной дисциплины «Настройка и использование программных средств InfoWatch» (код В) ..... 13
Рабочая программа учебной дисциплины «Подготовка и реализация Концепции Политики защиты данных» (код В) ..... 15
ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ..... 17
Формы аттестации ..... 17
Критерии оценки обучающихся ..... 18
Фонд оценочных средств ..... 20
ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ..... 30
Требования к квалификации педагогических кадров, представителей предприятий и организаций, обеспечивающих реализацию образовательного процесса ..... 30
Требования к материально-техническим условиям ..... 30
Требования к оборудованию слушателя для проведения занятий ..... 30
Требования к информационным и учебно-методическим условиям ..... 31

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая образовательная программа (далее – Программа) представляет собой совокупность требований, обязательных при реализации программы дополнительного профессионального образования повышения квалификации «Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы».

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 выполнения работ по разработке и реализации Политик защиты данных в системах защиты от утечки данных (DLP системы), а также оценки эффективности применения соответствующих Правил.

**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:** 40/4/1 (ак. час, нед., мес.).

**Режим занятии:** 32 академических часа самостоятельного обучения с использованием дистанционных образовательных технологий, 6 академических часов практического занятия с использованием средств видео-конференц-связи, 2 академических часа итоговой аттестации (зачета) с использованием средств видео-конференц-связи.

**Форма обучения**: заочная с применением дистанционных образовательных технологий

**Характеристика профессиональной деятельности слушателей**

Область профессиональной деятельности слушателей:

- обеспечение защиты данных от утечек

Специалист по защите данных от утечек готовится 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 |
| Дополнительные требования | Наличие сертификата «Специалист по использованию и администрированию InfoWatch Traffic Monitor 7» |

**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**

## ЗАЩИТА ДАННЫХ ОТ УТЕЧЕК. ОТ АНАЛИЗА БИЗНЕС-ПРОЦЕССОВ ДО НАСТРОЙКИ И ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМЫ.

**(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 (самосто-ятельная работа) | Внеауди-торная (самостоя-тельная работа) | Промежу-точная /итоговая аттеста-ция | |
| 1 | Обзор аналитических работ | 6,5 | 2,5 | 3,0 | 1,0 | Тестирование |
| 2 | Правовые и организационные аспекты легитимизации DLP системы | 3,8 | 1,3 | 2,0 | 0,5 | Тестирование |
| 3 | Настройка и использование программных средств InfoWatch | 10,1 | 5,6 | 4,0 | 0,5 | Тестирование |
| 4 | Подготовка и реализация Концепции Политики защиты данных | 17,6 | 0,4 | 11,2 | 6,0 | Лабораторный практикум |
| 5 | ИТОГОВАЯ АТТЕСТАЦИЯ | 2,0 | | | 2,0 | Зачет |
| | Всего: | 40,0 | 9,8 | 20,2 | 10,0 | |

**УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН**
**ПО**
**ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЕ**
**повышения квалификации**

**ЗАЩИТА ДАННЫХ ОТ УТЕЧЕК. ОТ АНАЛИЗА БИЗНЕС-ПРОЦЕССОВ ДО НАСТРОЙКИ И ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМЫ.**

**(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** | **Обзор аналитических работ** | **6,5** | **2,5** | **3,0** | **1,0** | **Тестирование** |
| 1.1 | Формирование плана аналитических работ и сбор требований | 1,0 | 0,5 | 0,5 | | |
| 1.2 | Анализ данных в DLP системе | 3,5 | 1,5 | 2,0 | | |
| 1.3 | Подготовка данных и формирование Концепции Политики защиты данных | 1,0 | 0,5 | 0,5 | | |
| | Тестирование | 1,0 | | | 1,0 | |
| **2** | **Правовые и организационные аспекты легитимизации DLP системы** | **3,8** | **1,3** | **2,0** | **0,5** | **Тестирование** |
| 2.1 | Нормативное обеспечение использования DLP системы | 1,7 | 0,7 | 1,0 | | |
| 2.2 | Организационное обеспечение использования DLP системы | 1,6 | 0,6 | 1,0 | | |
| | Тестирование | 0,5 | | | 0,5 | |
| **3** | **Настройка и использование** | **10,1** | **5,6** | **4,0** | **0,5** | **Тестирование** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **программных средств InfoWatch** | | | | | |
| 3.1 | Настройка и использование InfoWatch Traffic Monitor | 5,8 | 3,3 | 2,5 | | |
| 3.2 | Настройка и использование InfoWatch Device Monitor | 3,8 | 2,3 | 1,5 | | |
| | Тестирование | 0,5 | | | 0,5 | |
| **4** | **Подготовка и реализация Концепции Политики защиты данных** | **17,6** | **0,4** | **11,2** | **6,0** | **Лабораторный практикум** |
| 4.1 | Подготовка Концепции Политики защиты данных | 3,2 | 0,2 | 3 | | |
| 4.2 | Реализация Концепции Политики защиты данных | 0,4 | 0,2 | 0,2 | | |
| | Лабораторный практикум | 14,0 | | 8,0 | 6,0 | |
| **5** | **ИТОГОВАЯ АТТЕСТАЦИЯ** | **2,0** | | | **2,0** | **Зачет** |
| | **Всего:** | **40,0** | **9,8** | **20,2** | **10,0** | **-** |

## 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: 0,5-1,5 академических часа в день (кроме практического занятия 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 | Обзор аналитических работ | СР | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Правовые и организационные аспекты легитимизации DLP | СР | | | | | | | 1,0 | 1,0 | 1,0 | 1,0 | | | | | | | | | | | | | | | | | | | | |
| 3 | Настройка и использование программных средств Infowatch | СР | | | | | | | | | | | 1,0 | 1,0 | 1,5 | 1,0 | 1,0 | 1,5 | 1,0 | 1,0 | 1,0 | | | | | | | | | | | |
| 4 | Подготовка и реализация Концепции Политики защиты данных | СР | | | | | | | | | | | | | | | | | | | | 1,0 | 1,0 | 1,5 | 1,0 | 1,5 | 1,0 | 1,0 | 1,5 | 1,0 | 1,5 | 6,0 |
| 5 | Итоговая аттестация | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2,0 |

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

**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 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 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 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 | |
| **1.** | **Обзор аналитических работ** | **6,5** | **2,5** | **3,0** | **1,0** | **Тестирование** |
| 1.1 | Формирование плана аналитических работ и сбор требований | 1,0 | 0,5 | 0,5 | | |
| 1.2 | Анализ данных в DLP системе | 3,5 | 1,5 | 2,0 | | |
| 1.3 | Подготовка данных и формирование Концепции Политики защиты данных | 1,0 | 0,5 | 0,5 | | |
| | Тестирование | 1,0 | | | 1,0 | |

**Тема 1.1. Формирование плана аналитических работ и сбор требований**

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

**Тема 1.2. Анализ данных в DLP системе**

- Технологии анализа контента.
- Лингвистический анализ.

- Текстовые объекты.
- Эталонные документы.
- Бланки.
- Печати.
- Выгрузки из баз данных.
- Графические объекты.
- Автолигвист.

**Тема 1.3. 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.

**Структура и содержание дисциплины**

Общая трудоемкость дисциплины составляет 3,8 академических часа (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 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) | Промежу-точная /итоговая аттестация | |
| **2** | **Правовые и организационные аспекты легитимизации DLP системы** | **3,8** | **1,3** | **2,0** | **0,5** | **Тестирование** |
| 2.1 | Нормативное обеспечение использования DLP системы | 1,7 | 0,7 | 1,0 | | |
| 2.2 | Организационное обеспечение использования DLP системы | 1,6 | 0,6 | 1,0 | | |
| | Тестирование | 0,5 | | | 0,5 | |

**Тема 2.1. 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 2.2. 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.

**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 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 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 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 | |
| **3** | **Настройка и использование программных средств InfoWatch** | **10,1** | **5,6** | **4,0** | **0,5** | **Тестирование** |
| 3.1 | Настройка и использование InfoWatch Traffic Monitor | 5,8 | 3,3 | 2,5 | | |
| 3.2 | Настройка и использование InfoWatch Device Monitor | 3,8 | 2,3 | 1,5 | | |
| | Тестирование | 0,5 | | | 0,5 | |

**Тема 3.1. Настройка и использование InfoWatch Traffic Monitor**

- Вводная часть по настройке и администрированию ТМ.
- 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 3.2. Настройка и использование InfoWatch Device Monitor**

- Вводная часть по DM.
- Начало работы с Консолью управления DM.
- Алгоритм подготовки к созданию политики в консоли DM.
- 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 В)

**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 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 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 17,6 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала и выполнение лабораторного практикума) – 11,2 академических часов, практическое занятие с использованием средств видео-коференц-связи - 6 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 аттестация | |
| **4** | **Подготовка Концепции политики информационной безопасности** | **17,6** | **0,4** | **11,2** | **6,0** | **Лабораторный практикум** |
| 4.1 | Подготовка Концепции Политики защиты данных | 3,2 | 0,2 | 3 | | |
| 4.2 | Реализация Концепции Политики защиты данных | 0,4 | 0,2 | 0,2 | | |
| | Лабораторный практикум | 14,0 | | 8,0 | 6,0 | |

**Тема 4.1. Подготовка Концепции Политики защиты данных**

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

**Тема 4.2. Реализация Концепции Политики защиты данных**

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

## 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 «Повышение квалификации «Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы 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:**<br>- Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес.<br>- Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их | **Специалист должен обладать профессиональными компетенциями (ПК), соответствующими основным видам профессиональной деятельности:**<br>- Выполнение установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования | **Знания:**<br>- Принципы формирования политики информационной безопасности в автоматизированных системах<br>- Программно-аппаратные средства защиты информации автоматизированных систем<br>- Принципы организации и структура систем защиты программного обеспечения автоматизированных систем<br>- Нормативные правовые акты в области защиты информации |

| | | |
|---|---|---|
| эффективность и качество.<br>- Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.<br>- Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.<br>- Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.<br>- Ориентироваться в условиях частой смены технологий в профессиональной деятельности.<br>- Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий | автоматизированной системы<br>- Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации<br>- Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы<br>- Выявление угроз безопасности информации в автоматизированных системах<br>- Принятие мер защиты информации при выявлении новых угроз безопасности информации<br>- Анализ недостатков в функционировании системы защиты информации автоматизированной системы<br>- Устранение недостатков в функционировании системы защиты информации автоматизированной системы | - Организационные меры по защите информации<br>**Умения:**<br>- Формировать политику безопасности программных компонентов автоматизированных систем<br>- Регистрировать события, связанные с защитой информации в автоматизированных системах<br>- Анализировать события, связанные с защитой информации в автоматизированных системах<br>- Классифицировать и оценивать угрозы информационной безопасности<br>- 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.<br>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.<br>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 «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 в 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 ТМ (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 IW TM (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 IW Traffic Monitor к специальным техническим средствам, предназначенным 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? (Выберите несколько вариантов ответа)
   - Расширенный.
   - Обычный.
   - Детальный.
   - Пользовательский.

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

3. Как определяется время перехвата события? (Выберите несколько вариантов ответа)
   - Время перехвата события - это локальное время на агенте Device Monitor, где осуществляется перехват.
   - Время перехвата события - это локальное время на сервере Device Monitor.
   - Время перехвата события - это локальное время на сервере 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 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 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 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».

## ЛАБОРАТОРНЫЙ ПРАКТИКУМ

### Дисциплина «Подготовка и реализация Концепции Политики защиты данных»

### Разработка и реализация 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 Device Monitor**

перечислить правила, которые должны быть созданы в системе 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. Методы сбора требований: перечень, возможности, особенности использования.
2. Метод сбора требований – интервью, возможности и ограничения метода, способы повышения эффективности использования.
3. Метод сбора требований – опросный лист, возможности и ограничения метода, способы повышения эффективности использования.
4. Метод сбора требований – изучение документации, возможности и ограничения метода, способы повышения эффективности использования.
5. Организация процесса сбора требований.
6. Технология «Лингвистический анализ»: назначение, возможности, принципы работы.
7. Технология «Текстовые объекты»: назначение, возможности, принципы работы.
8. Технология «Эталонные документы»: назначение, возможности, принципы работы.
9. Технология «Бланки»: назначение, возможности, принципы работы.
10. Технология «Печати»: назначение, возможности, принципы работы.
11. Технология «Выгрузки из баз данных»: назначение, возможности, принципы работы.
12. Технология «Графические объекты»: назначение, возможности, принципы работы.
13. Технология «Автолигвист»: назначение, возможности, принципы работы.
14. Порядок подготовки данных для формирования Политики защиты данных
15. Содержание и элементы Политики защиты данных.
16. Федеральное законодательство РФ в сфере защиты информации.
17. Ответственность сотрудников за утечку данных.
18. Порядок привлечения к ответственности сотрудников, виновных в утечке данных.
19. Организационное обеспечение использования системы защиты от утечки данных.
20. 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 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=179347699
2. InfoWatch Traffic Monitor Руководство пользователя. https://kb.InfoWatch.com/pages/viewpage.action?pageId=179348183
3. InfoWatch Device Monitor. Руководство пользователя https://kb.InfoWatch.com/pages/viewpage.action?pageId=173407089


## 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