МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

РАССМОТРЕНО
На заседании ПЦК МиЕНД
Протокол заседания
№ 07 от «31» августа 2022 г.
_____ Бойко Я.С

УТВЕРЖДАЮ
Зам. директора по УВР
НефтИн (филиал) ФГБОУ ВО «ЮГУ»
«31» августа 2022 г.
_____Хайбулина Р.И

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

КОМПЛЕКТ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ МАТЕРИАЛОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

(МЕЖДИСЦИПЛИНАРНОМУ КУРСУ)

МДК.02.03 КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
(наименование учебной дисциплины, МДК)

программы подготовки специалистов среднего звена (ППССЗ)

по специальности СПО

10.02.05 Обеспечение информационной безопасности автоматизированных систем
(код, наименование)
программы подготовки специалистов среднего звена (ППССЗ)

базовой подготовки

г. Нижневартовск

-2022-

Комплект контрольно-измерительных материалов по учебной дисциплине МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности программы подготовки специалистов среднего звена (ППССЗ) разработан на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, в соответствии с рабочей программой учебной дисциплины МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности.

Разработчики:

НефтИн (филиал) ФГБОУ ВО «ЮГУ»	преподаватель	А.Н. Тымощук
(место работы)	(занимаемая должность)	(инициалы, фамилия)
НефтИн (филиал) ФГБОУ ВО «ЮГУ»	преподаватель	А.Г. Баталкина
(место работы)	(занимаемая должность)	(инициалы, фамилия)

1. Паспорт комплекта контрольно-измерительных материалов

1.1. Область применения

Комплект контрольно-измерительных материалов предназначен для проверки результатов освоения учебной дисциплины (далее - УД) МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности программы подготовки специалистов среднего звена (ППССЗ) по специальности СПО *10.02.05 Обеспечение информационной безопасности автоматизированных систем.*

Комплект контрольно-измерительных материалов позволяет оценивать:

1.1.1. Освоение профессиональных компетенций (ПК) и общих компетенций (ОК)

Профессиональные и общие компетенции	Средства проверки (№ задания)
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	ПЗ 1-52, Выполнение практических работ
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	ПЗ 1-52, Выполнение практических работ
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	ПЗ 1-52, Выполнение практических работ
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	ПЗ 1-52, Выполнение практических работ
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	ПЗ 1-52, Выполнение практических работ
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-	ПЗ 1-52, Выполнение практических работ

аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	ПЗ 1-52, Выполнение практических работ
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	ПЗ 1-52, Выполнение практических работ
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	ПЗ 1-52, Выполнение практических работ
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	ПЗ 1-52, Выполнение практических работ
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	ПЗ 1-52, Выполнение практических работ
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	ПЗ 1-52, Выполнение практических работ
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	ПЗ 1-52, Выполнение практических работ
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	ПЗ 1-52, Выполнение практических работ
ОК 09. Использовать	ПЗ 1-52,

информационные технологии в профессиональной деятельности.	Выполнение практических работ
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	ПЗ 1-52, Выполнение практических работ

1.1.2. Освоение умений и усвоение знаний

Освоенные умения, усвоенные знания	№ заданий для проверки
1	2
У1: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	ПЗ 1-52
У2: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;	ПЗ 1-52
У3: проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	ПЗ 1-52
З1: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	ПЗ 1-52
З2: методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	ПЗ 1-52
З3: типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;	ПЗ 1-52

(Освоенные умения и усвоенные знания перечисляются из части ФГОС соответствующей УД (МДК), при наличии здесь указываются и дополнительные умения, и знания, введенные за счёт вариативной части).
Номера заданий для проверки – номера методических указаний к выполнению ЛПЗ, номера заданий в методические указания в ЛПЗ)

1.2. Система контроля и оценки освоения программы учебной дисциплины МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности.

1.2.1. Формы промежуточной аттестации по ППССЗ при освоении учебной дисциплины МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности.

Учебная дисциплина (междисциплинарный курс)	Формы промежуточной аттестации
1	2
МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности 7 семестр	Дифференцированный зачет

(Формы промежуточной аттестации указываются в соответствии с учебным планом)

1.2.2. Организация контроля и оценки освоения программы учебной дисциплины МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности.

Промежуточный контроль по дисциплине осуществляется форме дифференцированного зачета.

Условием положительной аттестации по дисциплине на дифференцированном зачёте является положительная оценка освоения всех умений, знаний, а также формируемых профессиональных компетенций по всем контролируемым показателям.

2. Комплект материалов для оценки уровня освоения умений и усвоения знаний, сформированности общих и профессиональных компетенций при изучении учебной дисциплины МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности.

2.1. Комплект материалов для оценки уровня освоения умений, усвоения знаний, сформированности общих и профессиональных компетенций

ТЕМЫ РЕФЕРАТОВ (ДОКЛАДОВ)

по учебной дисциплине МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности.

1. Конфигурация сетевой инфраструктуры.
2. Корпоративная защита от внутренних угроз.
3. Организация подготовки кадров и повышения квалификации в области обеспечения информационной безопасности.
4. Корпоративная нормативная база по защите информации.
5. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности
6. Требования к полноте эффективных стандартов по безопасности.
7. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.
8. Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия).
9. Нормативно-методические документы по обеспечению безопасности информации.
10. Аудит программного кода по требованиям безопасности
11. Назначение, функции и типы систем видеозащиты
12. Информационная безопасность: экономические аспекты
13. Оценка безопасности автоматизированных систем
14. Функциональная безопасность программных средств
15. Утечки информации: как избежать
16. Методы борьбы с фишинговыми атаками
17. Законодательство о персональных данных
18. Современные угрозы и защита электронной почты
19. Защита от внутренних угроз

Критерии оценки:

Оценка «5» ставится, если:

• Содержание реферата соответствует теме;

• Тема раскрыта полностью;

• Оформление реферата соответствует принятым стандартам;

• При работе над рефератом автор использовал современную литературу;

• В реферате отражена практическая работа автора по данной теме;

• В сообщении автор не допускает ошибок, но допускает оговорки по невнимательности, которые легко исправляет по требованию учителя;

• Сообщение логично, последовательно, технически грамотно;

• На дополнительные вопросы даются правильные ответы,

Оценка «4» ставится, если:

• Содержание реферата соответствует теме;

• Тема раскрыта полностью;

• Оформление реферата соответствует принятым стандартам;

• При работе над рефератом автор использовал современную литературу;

• В реферате отражена практическая работа автора по данной теме;

• В сообщении автор допускает одну ошибку или два-три недочета, допускает неполноту

ответа, которые исправляет только с помощью учителя.

Оценка «3» ставится, если:

• Содержание реферата не полностью соответствует теме;

• Тема раскрыта недостаточно полно;

• В оформлении реферата допущены ошибки;

• Литература, используемая автором, при работе над рефератом устарела;

• В реферате не отражена практическая работа автора по данной теме;

• Сообщение по теме реферата допускаются 2-3 ошибки;

• Сообщение неполно, построено несвязно, но выявляет общее понимание работы;

• При ответе на дополнительные вопросы допускаются ошибки, ответ неуверенный, требует постоянной помощи учителя.

Оценка «2» ставится, если:

• Содержание реферата не соответствует теме;.

Оценка «1» ставится, если:

• Обучающийся не представил рефератную работу соответствующую выбранной теме.

Составители _____ /А.Г. Баталкина /
подпись Ф.И.О.
__.__.2022 г.

_____ /А.Н Тымощук /
подпись Ф.И.О.
__.__.2022 г.

КОМПЛЕКС ПРАКТИЧЕСКИХ ЗАНЯТИЙ
по учебной дисциплине МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности.

ТЕМАТИКА ПРАКТИЧЕСКИХ ЗАНЯТИЙ

№	Название практического занятия	Кол-во часов
1.	Организация безопасной, аккуратной и эффективной рабочей зоны	2
2.	Организация безопасной, аккуратной и эффективной рабочей зоны	2
3.	Планирование работы специалиста по информационной безопасности в соответствии с изменяющимися приоритетами	2
4.	Планирование работы специалиста по информационной безопасности в соответствии с изменяющимися приоритетами	2
5.	Конфигурация сетевой инфраструктуры: настройка хост-машины, сетевого окружения, виртуальных машин	2
6.	Конфигурация сетевой инфраструктуры: настройка хост-машины, сетевого окружения, виртуальных машин	2
7.	Установка и настройка системы корпоративной защиты от внутренних угроз	2
8.	Установка и настройка системы корпоративной защиты от внутренних угроз	2
9.	Запуск системы, проверка функциональности и соответствия настроек целевой сетевой инфраструктуре	2
10.	Запуск системы, проверка функциональности и соответствия настроек целевой сетевой инфраструктуре	2
11.	Имитация процесса утечки конфиденциальной информации в системе	2
12.	Имитация процесса утечки конфиденциальной информации в системе	2
13.	Имитация процесса утечки конфиденциальной информации в системе	2
14.	Настройка работоспособности системы и отчет по оценке работоспособности системы	2
15.	Настройка работоспособности системы и отчет по оценке работоспособности системы	2
16.	Настройка работоспособности системы и отчет по оценке работоспособности системы	2
17.	Настройка работоспособности системы и отчет по оценке работоспособности системы	2
18.	Разработка и применение политики агентского мониторинга для работы с носителями и устройствами	2
19.	Разработка и применение политики агентского мониторинга для работы с носителями и устройствами	2
20.	Разработка и применение политики агентского мониторинга для работы с носителями и устройствами	2
21.	Разработка и применение политики агентского мониторинга для работы с носителями и устройствами	2
22.	Разработка и применение политики агентского мониторинга для работы с носителями и устройствами	2
23.	Разработка и применение политики агентского мониторинга для работы с файлами	2
24.	Разработка и применение политики агентского мониторинга для работы с файлами	2
25.	Разработка и применение политики агентского мониторинга для работы с файлами	2

26.	Разработка и применение политики агентского мониторинга для работы с файлами	2
27.	Разработка и применение политики агентского мониторинга для работы с файлами	2
28.	Работа с исключениями из перехвата	2
29.	Работа с исключениями из перехвата	2
30.	Работа с исключениями из перехвата	2
31.	Разработка политики безопасности, перекрывающей каналы передачи персональных данных сотрудников и контрагентов по электронной почте	2
32.	Разработка политики безопасности, перекрывающей каналы передачи персональных данных сотрудников и контрагентов по электронной почте	2
33.	Разработка политики безопасности, перекрывающей каналы передачи базы клиентов организации в архиве с использованием файловых протоколов	2
34.	Разработка политики безопасности, перекрывающей каналы передачи базы клиентов организации в архиве с использованием файловых протоколов	2
35.	Разработка политики безопасности, перекрывающей каналы передачи информации, составляющейкоммерческую тайну.	2
36.	Разработка политики безопасности, перекрывающей каналы передачи информации, составляющейкоммерческую тайну.	2
37.	Разработка политики безопасности, перекрывающей каналы передачи информации, составляющейкоммерческую тайну.	2
38.	Разработка политики безопасности, перекрывающей каналы передачи информации, составляющей коммерческую тайну	2
39.	Разработка политики безопасности, перекрывающей каналы передачи информации, составляющей коммерческую тайну	2
40.	Разработка политики безопасности, перекрывающей каналы передачи информации, составляющей коммерческую тайну	2
41.	Занесение политики информационной безопасности в DLP-систему	2
42.	Занесение политики информационной безопасности в DLP-систему	2
43.	Модификация объекты защиты, категории, технологии защиты в DLP-системе	2
44.	Модификация объекты защиты, категории, технологии защиты в DLP-системе	2
45.	Применение политики для контроля трафика, выявления и блокирования инцидентов безопасности	2
46.	Применение политики для контроля трафика, выявления и блокирования инцидентов безопасности	2
47.	Интерфейс управления системы корпоративной защиты информации IWTM	2
48.	Интерфейс управления системы корпоративной защиты информации IWTM	2
49.	Механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов	2
50.	Механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов	2
51.	Детализированные отчёты о нарушениях	2
52.	Классификация уровня угрозы инцидента	2
		104

Практическое занятие № 1 -2

Тема: Организация безопасной, аккуратной и эффективной рабочей зоны.

Цель: изучить общие требования к организации рабочего места, изучить требования к безопасному содержанию рабочего места, составить рабочую зону для предприятия.

Теоретическая часть: (изучить)

Общие требования к организации безопасного рабочего места

I. Общие положения

1. Общие требования к организации безопасного рабочего места (далее – Требования) разработаны в целях обеспечения выполнения требований охраны труда работниками, занятыми на своих рабочих местах. Для рабочих мест с территориально меняющимися рабочими зонами, где рабочей зоной считается оснащенная необходимыми средствами производства часть рабочего места, в которой один работник или несколько работников выполняют схожие работы или технологические операции 1 положения Требований распространяются на каждую рабочую зону.

2. Рабочее место, его оборудование и оснащение, применяемые в соответствии с особенностями выполняемых работ, должны обеспечивать безопасность, охрану здоровья и работоспособность занятых на нем работников.

3. На рабочем месте (в рабочей зоне) должны быть приняты меры по снижению, по возможности, до установленных предельно допустимых значений уровней воздействия (концентрации) вредных и (или) опасных производственных факторов на занятых на данном рабочем месте работников с учетом применения ими средств индивидуальной (коллективной) защиты.

4. Рабочее место (рабочая зона), его размеры, взаимное расположение органов управления, средств отображения информации, размещение вспомогательного оборудования и инструментов должны соответствовать антропометрическим, физиологическим и психофизиологическим свойствам занятых на нем работников и особенностям выполняемой работы.

II. Требования к организации рабочего места

5. При организации рабочего места (рабочей зоны) должна быть обеспечена возможность смены рабочей позы занятыми на нем работниками.

6. В зависимости от особенностей выполняемой работы рабочая поза работника «сидя» является более удобной, чем рабочая поза «стоя». Если основной рабочей позой работника является положение «стоя», необходимо обеспечить периодическое чередование данной рабочей позы с положением «сидя», в том числе посредством организации места для сидения.

7. Удобство рабочей позы работника в положении «сидя» достигается регулированием взаимного положения места для сидения и рабочей поверхности, в том числе ее высоты и размеров, а также высоты и угла наклона подставки для ног при ее применении. При невозможности обеспечения указанного выше регулирования рабочей позы допускается использование рабочего места с нерегулируемыми параметрами. В этом случае высоту рабочей поверхности устанавливают, исходя из особенностей выполнения работы, требований к сенсорному контролю и обеспечению требуемой точности действий, среднего роста работающих (мужчин - если работают только мужчины, женщин - если работают только женщины, по-отдельности мужчин и женщин - если работают и мужчины, и женщины).

8. При организации рабочего места (рабочей зоны) должно быть обеспечено выполнение трудовых операций в зонах «моторного поля» - зонах оптимальной, легкой

досягаемости и возможной досягаемости, в зависимости от требуемой точности и частоты действий.

9. При организации рабочего места (рабочей зоны) должно быть обеспечено устойчивое положение и свобода движений занятого на нем работника, сенсорный контроль деятельности и безопасность выполнения трудовых операций.

10. При организации рабочего места (рабочей зоны) должны быть исключена или снижена до минимума продолжительность выполнения работы в неудобных 2 и вынужденных 3 позах (характеризующихся, например, необходимостью сильно наклоняться вперед или в стороны, приседать, работать с вытянутыми или высоко поднятыми руками, закинув голову назад), вызывающих повышенную утомляемость.

11. При организации рабочего места (рабочей зоны) необходимо обеспечить необходимый обзор наблюдения с места выполнения работ зоны информационного поля, визуальных средств отображения информации, знаков безопасности.

12. Средства отображения информации должны быть размещены в зонах информационного поля рабочего места с учетом частоты и значимости поступающей информации, типа средства отображения информации, точности и скорости слежения и считывания.

13. Визуальные средства отображения информации должны быть освещены в соответствии с нормативами и достаточно для восприятия отображаемой информации с места выполнения работ.

14. Органы управления машинами и оборудованием должны быть размещены на рабочем месте (в рабочей зоне) с учетом рабочей позы работника, функционального назначения органа управления, частоты применения, последовательности использования, функциональной связи с соответствующими средствами отображения информации.

15. Расстояние между органами управления машинами и оборудованием должно исключать возможность произвольного изменения положения не задействованного органа управления при манипуляции с иным смежным органом управления.

16. Участки и зоны, где возможно травмирование работника, должны быть обозначены сигнальными цветами и знаками безопасности.

17. Применение знаков безопасности не заменяет необходимости информирования работника всеми доступными способами, которые могут предупредить или уменьшить вредное или опасное воздействие на работников.

18. Рабочее место (рабочая зона), при необходимости, оснащается вспомогательным подъемно-транспортным оборудованием (средствами).

19. Цветовое оформление зон рабочего места должно соответствовать требованиям технической эстетики.

20. При организации рабочих мест их взаимное расположение и компоновка должны обеспечивать безопасный доступ занятых на них работников на каждое рабочее место и возможность быстрой эвакуации работников при возникновении аварийной или иной чрезвычайной ситуации. Пути эвакуации и проходы должны быть обозначены соответствующими указателями и иметь достаточную освещенность.

III. Требования к безопасному содержанию рабочего места

21. Рабочее место (рабочая зона) и взаимное расположение его элементов должны обеспечивать безопасное и удобное содержание, в том числе техническое обслуживание, уборку и чистку используемых на рабочем месте машин и оборудования, инструментов и мебели.

22. Организация и содержание рабочих мест, а также расстояния между рабочими местами должны обеспечивать безопасное передвижение работников и транспортных

средств, удобные и безопасные действия с сырьем, материалами, заготовками, полуфабрикатами.

23. Работники должны выполнять следующие процедуры по содержанию своих рабочих мест (рабочих зон): - сортировку; - самоорганизацию; - систематическую уборку (содержание в чистоте).

24. При сортировке выполняется разделение предметов, включая инструменты, сырье и материалы, на являющиеся и не являющиеся источниками опасностей, на необходимые при выполнении конкретных работ на рабочем месте (в рабочей зоне) и не требующиеся при выполнении этих работ с последующей уборкой с рабочего места инструментов, сырья и материалов, не требующихся при выполнении указанных работ перед началом их выполнения.

25. При самоорганизации рабочего места (рабочих зон) обеспечивается соблюдение порядка на нем путем размещения на рабочем месте или в рабочей зоне при выполнении конкретных работ только необходимых для этого предметов, включая инструменты, сырье и материалы, таким образом, чтобы максимально снизить риски реализации опасностей и получения микротравм при их использовании. При хранении предметов, включая инструменты сырье и материалы, на рабочем месте необходимо обязательно применять различные методы визуализации, такие как оконтуривание, маркировка, разметка, цветовое кодирование и другие аналогичные методы. 5

26. При систематической уборке (содержании в чистоте) обеспечивается постоянное поддержание рабочих мест (рабочих зон) с расположенными в них машинами, оборудованием, иными предметами, включая инструменты, сырье и материалы, в чистоте и постоянной готовности к использованию путем удаления отходов производства, например, стружки, опилок, окалины, пролитых технологических жидкостей и реагентов, пыли, мусора, использованной упаковки с рабочего места, а также размещения отходов в предназначенные для этого контейнеры.

27. Процедуры по содержанию рабочего места (рабочих зон) в соответствии с пунктом 23 Требований следует документировать в локальных нормативных актах работодателя в рамках Системы управления охраной труда (при наличии) или иных документах работодателя, например, инструкциях по охране труда.

28. Работодатель должен обеспечить процесс непрерывного совершенствования, поддержания и развития результатов, достигнутых при выполнении пунктов 23 и 27 Требований.

Практическое задание:

На основе изученных выше требований к безопасному содержанию рабочего места, составить рабочую зону для предприятия.

Практическое занятие № 3-4.

Тема: Планирование работы специалиста по информационной безопасности в соответствии с изменяющимися приоритетами.

Цель: изучить проблемы информационной безопасности, разработать план мероприятий, обеспечивающий минимизацию информационных рисков по направлениям.

Теоретическая часть:

Проблемы информационной безопасности: алгоритм построения системы ИБ с нуля.

1. Заручиться поддержкой руководства.

Если отдел информационной безопасности создан по инициативе руководства компании, то проблема решена. Однако в реальности часто ИБ-отдел создается стихийно, при этом существует служба безопасности, которая не очень понимает, что такое

технические меры защиты, есть также ИТ-служба, которая воспринимает ИБ-отдел как помеху и т д.

Организация защиты информации на практике ведется одним из способов: «снизу вверх» либо «сверху вниз».

Подход «снизу вверх» наиболее распространен. В данном случае инициатива по всем ИБ-мероприятиям исходит от рядовых специалистов или линейных руководителей. Подход включает в себя написание служебных записок, доведение до руководства информации об инцидентах и прочее. Такой подход малоэффективен, так как высшее руководство компании не до конца понимает целесообразность и необходимость проведения большинства работ по информационной безопасности. В итоге информационной безопасности уделяется малое внимание, ей занимаются по остаточному принципу, работы зачастую носят несистемный характер.

Подход «сверху вниз» предполагает вовлеченность топ-менеджмента и владельцев бизнеса в проблематику информационной безопасности. Данный подход считается более эффективным, поскольку руководство смотрит на информационную безопасность с позиции бизнеса, ведется оценка рисков. Подход позволяет получать требуемые ресурсы и принимать необходимые меры, так как комплексная защита информации на предприятии — инициатива руководства.

На первом этапе следует заручиться поддержкой руководства, а в организации работ придерживаться подхода «сверху вниз».

2. Определить состав рабочей группы.

Важно определить, какие специалисты будут принимать активное участие в работах по информационной безопасности.

Есть мнение, что можно отдать работы по ИБ на аутсорсинг и полностью сосредоточиться на текущих задачах. Это верно лишь отчасти, поскольку никакие внешние эксперты не смогут оценить реальную важность и ценность информационных ресурсов компании, они могут лишь привнести объективный взгляд со стороны. Поэтому в рабочей группе обязательно должен быть представитель владельца информационных ресурсов.

3. Определить риски.

После того как сформирована рабочая группа и получена поддержка действий от руководства, переходим к этапу управления рисками. На этом этапе необходимо:

- идентифицировать информационные активы, представляющие ценность;
- провести анализ информационных ресурсов, к защите которых предъявляются требования со стороны законодательства/отрасли;
- провести анализ информационных ресурсов на существующие уязвимости с точки зрения информационной безопасности;
- провести анализ источников угроз;
- проанализировать сами угрозы;
- оценить возможный ущерб;
- подготовить отчет для презентации руководству.

После проведения этапа должен быть составлен список определенных угроз и оценен ущерб, который может быть потенциально нанесен компании при реализации этих угроз. При расчете ущерба следует учитывать вероятность наступления тех или иных угроз.

После оценки возможного ущерба необходимо проработать риски по каждой актуальной угрозе.

4. Принять организационные меры.

На данном этапе разрабатываются политики, стандарты, руководства и инструкции, направленные на поддержание системы ИБ. Фиксируется ответственность сотрудников за нарушение требований ИБ, разглашение и нарушение конфиденциальности информации. Важно понимать, что эффективная система ИБ не может существовать без регламентов, инструкций, документов, направленных на ее поддержание.

5. Выбрать и внедрить меры и средства защиты информации.

На этом этапе осуществляется выбор средств защиты информации и оценка их эффективности. Оценка эффективности нужна для понимания, окупятся ли затраты, потраченные на СЗИ. Прибыль здесь косвенная — минимизация рисков, которые были определены ранее.

При выборе мер и средств защиты необходимо руководствоваться правилом: затраты на приобретение, внедрение, настройку, обучение специалистов, сопровождение средств защиты не должны превышать ущерба от реализации угрозы, на защиту от которой эти средства направлены.

6. Довести информацию до заинтересованных лиц.

Важно донести до пользователей необходимую информацию по ИБ доступными для них способами. Сотрудникам лучше всего показать на практике, как безопасно работать и взаимодействовать, провести презентацию или обучение. Руководству полезно будет показать убытки, которые может получить компания в случае невыполнения мер по информационной безопасности. Специалистам нужно показать, какими средствами можно пользоваться, а какими нет и почему, а также озвучить ответственность за нарушения этих мер.

7. Провести мониторинг и оценку.

После проведения всех этапов необходимо провести мониторинг и оценку результатов работ. Важно понять, насколько изменилось состояние ИБ.

Например, хорошим показателем будет появление инцидентов или вопросов по ИБ после проведения обучения сотрудников. Если до обучения обращений по инцидентам не возникало, а после обучения стали появляться инциденты, значит, оно прошло не зря.

Но на этом работа не заканчивается. Цикличность работ по ИБ связана с тем, что информационная среда очень изменчива. Происходят изменения внутри самих информационных активов, изменения в информационных технологиях, в способах обработки информации, а значит, нужно снова возвращаться к анализу рисков и актуализации системы ИБ.

Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников Департамента и подведомственных учреждений в области информационной безопасности возлагается на администратора информационной безопасности. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности». Обучение сотрудников Департамента правилам обращения с конфиденциальной информацией, проводится путем:

- проведения администратором информационной безопасности инструктивных занятий с сотрудниками, принимаемыми на работу в Департамент;
- самостоятельного изучения сотрудниками внутренних нормативных документов Департамента.

Допуск сотрудников к работе с защищаемыми информационными ресурсами Департамента осуществляется только после его ознакомления с настоящими Регламентом. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками Департамента, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

Практическое задание:

«Разработка плана мероприятий по защите информации на предприятии»

Разработать план мероприятий, обеспечивающий минимизацию информационных рисков по трём направлениям:

- организационно-правовые мероприятия;
- обеспечение физической защиты информации;
- внедрение программно - аппаратных средств защиты информации.

Практическое занятие № 5-6

Тема: Конфигурация сетевой инфраструктуры: настройка хост – машины, сетевого окружения, виртуальных машин.

Цель: научиться включать на сервере программу Удаленный рабочий стол для администрирования; включать пользователей в соответствующую группу, чтобы разрешить им удаленно администрировать сервер; подключаться к серверу с помощью программы Удаленный рабочий стол для администрирования.

Теоретическая часть:

В семействе Windows Server был впервые реализован тесно интегрированный набор программных средств и технологий, позволяющих выполнять удаленное администрирование и совместно использовать приложения с помощью Служб терминалов (Terminal Services).

Эволюция продолжилась: отныне службы терминалов — неотъемлемый компонент семейства Windows Server, а инструмент Дистанционное управление рабочим столом (Remote Desktop) усовершенствован и позиционируется как стандартная функция. Так что теперь достаточно одного щелчка мыши, и компьютер с Windows Server будет параллельно обрабатывать до двух подключений удаленного администрирования. Добавив компонент Сервер терминалов (Terminal Server) и настроив соответствующую лицензию, администратор добьется еще большего эффекта: множество пользователей смогут запускать приложения на сервере. На этом занятии вы научитесь работать со служебной программой Удаленный рабочий стол для администрирования (Remote Desktop for Administration).

Включение и конфигурирование программы Удаленный рабочий стол для администрирования.

Службы терминалов позволяют совместно использовать приложения с помощью таких инструментов, как Дистанционное управление рабочим столом (Remote Desktop), Удаленный помощник (Remote Assistance) и Сервер терминалов (Terminal Server). По умолчанию служба устанавливается вместе с Windows Server и настраивается в программе Дистанционное управление рабочим столом для работы в режиме удаленного администрирования: допускает только два параллельных удаленных подключения и не содержит компоненты для совместного использования приложений из состава Сервера терминалов. Следовательно, Дистанционное управление рабочим столом создает очень небольшую дополнительную нагрузку на систему, причем не требует дополнительного лицензирования.

Примечание Поскольку Службы терминалов и Дистанционное управление рабочим столом являются стандартными компонентами Windows Server, каждый сервер способен поддерживать удаленные подключения к своей консоли. Термин «сервер терминалов», таким образом, теперь по праву можно применить к любому компьютеру под управлением Windows Server, обеспечивающему совместное использование приложений несколькими клиентами за счет добавления компонента Службы терминалов.

Другие компоненты — Сервер терминалов и службу Лицензирование сервера терминалов (Terminal Server Licensing) — нужно добавлять с помощью функции Установка и удаление программ (Add Or Remove Programs). Тем не менее, все средства администрирования для настройки и поддержки клиентских подключений и управления сервером терминалов устанавливаются по умолчанию на все компьютеры с Windows Server.

Эти средства и их функции описаны в таблице 1.

Таблица 1. Стандартные компоненты *Сервер терминалов* и *Подключение к удаленному рабочему столу*

Установленное ПО	Назначение
Настройка служб терминалов (Terminal Services Configuration)	Настройка свойств сервера терминалов, в том числе параметров сеанса, сети, клиентского рабочего стола и удаленного управления клиентом
Диспетчер служб терминалов (Terminal Services Manager)	Отправка сообщений клиентам, подключенным к серверу терминалов, отключение или завершение сеансов, а также инициирование удаленного управления или маскировки сеансов
*Подключение к удаленному рабочему столу (*Установочные файлы клиента Remote Desktop Connection)	Установка клиентского приложения *Дистанционное управление рабочим столом* (Remote Desktop) для Windows Server 2003 или Windows XP. 32_разрядное клиентское ПО *Дистанционное управление рабочим столом* устанавливается в папку %Systemroot%\System32\ Clients\Tsclient\Win32 на сервере терминалов
Лицензирование служб терминалов (Terminal Services Licensing)	Настройка лицензий для клиентских подключений к серверу терминалов. Это средство не подходит для сред, где используется только *Удаленный рабочий стол для администрирования*

Чтобы разрешить подключения Дистанционное управление рабочим столом (Remote Desktop) на компьютере под управлением Windows Server, в Панели управления выберите Система (System Properties). На вкладке Удаленное использование (Remote) выберите Разрешить удаленный доступ к этому компьютеру (Allow Users To Connect Remotely To This Computer).

Примечание: если сервер терминалов является контроллером домена, необходимо

также настроить групповую политику контроллера, чтобы разрешить группе Пользователи удаленного рабочего стола (Remote Desktop Users) подключение посредством служб терминалов. На серверах, не являющихся контроллерами домена, подключение через службы терминалов пользователям из этой группы разрешено по умолчанию.

Подключение к удаленному рабочему столу.

Подключение к удаленному рабочему столу (Remote Desktop Connection) — это клиентское приложение, используемое для подключения к серверу в контексте режима Дистанционное управление рабочим столом (Remote Desktop) или Сервер терминалов (Terminal Server). Для клиента нет функциональных различий между этими двумя конфигурациями сервера.

На компьютерах с Windows XP и Windows Server 2003 программа Подключение к удаленному рабочему столу установлена по умолчанию, но глубоко запрятана:

Пуск (Start)\Все программы (All Programs)\ Стандартные (Accessories)\Связь

(Communications)\Подключение к удаленному рабочему столу (Remote Desktop Connection).

На других платформах программу Подключение к удаленному рабочему столу можно установить с компакт_диска Windows Server либо из установочной папки клиента (%Systemroot%\System32\Clients \Tsclient\Win32) на любом из компьютеров под управлением Windows Server. Установочный пакет MSI можно распространять на системы Windows с помощью групповой политики или средствами SMS (Systems Management Server).

Совет: рекомендуется обновить предыдущие версии клиента Служб терминалов, установив последнюю версию Подключение к удаленному рабочему столу, чтобы обеспечить наиболее оптимальную, безопасную и стабильную среду, поскольку в этом случае будет доступен улучшенный пользовательский интерфейс, 128_битное шифрование и выбор альтернативных портов.

Настройка клиента удаленного подключения к рабочему столу.

Вы можете управлять множеством аспектов дистанционного подключения как со стороны клиента, так и со стороны сервера. В таблице 2 перечислены конфигурационные параметры и их назначение.

Таблица 2. Параметры программы *Удаленное подключение к рабочему столу*

Параметры	Назначение
Параметры клиента	
Общие (General)	Параметры выбора компьютера, к которому необходимо подключаться, настройка статических реквизитов для входа в систему, а также сохранение параметров для данного подключения
Экран (Display)	Задает размер окна клиента, глубину цвета, а также доступность панели подключений при работе в полноэкранном режиме
Локальные ресурсы (Local Resources)	Параметры передачи звуковых событий на локальный компьютер, помимо стандартных выходных сигналов мыши, клавиатуры и экрана. Также параметры на этой вкладке определяют, как удаленный компьютер интерпретирует комбинации клавиш Windows (например Alt+Tab), и доступны ли в сеансе удаленного доступа такие устройства, как локальные диски, принтеры и последовательные порты
Программы (Programs)	Задает путь и папки расположения для любых программ, которые необходимо запустить после установки соединения
Дополнительно (Experience)	Категории функций экрана можно включать или отключать в зависимости от пропускной способности канала связи между локальным и удаленными компьютерами. Предусмотрены параметры для отображения фона рабочего стола, содержимого окна при перетаскивании, визуальных эффектов при прорисовке меню и окон, тем рабочего стола; также вы можете активировать режим кэширования растровой графики, при котором после каждого интервала обновления передаются только изменения, а не весь экран целиком
Параметры сервера	
Параметры входа (Logon Settings)	Позволяет задать статические реквизиты для подключения вместо реквизитов, предоставляемых клиентом
Сеансы (Sessions)	Чтобы перекрыть настройки клиента, задайте здесь параметры завершения прерванного сеанса, ограничения длительности сеанса и времени его простоя, а также допустимость повторного подключения
Среда (Environment)	Перекрывает настройки из профиля пользователя для данного подключения в отношении запуска программы: здесь вы можете переопределить запускаемую при подключении программу. Заданный здесь путь и папка запуска приоритетнее настроек, сделанных программой *Подключение к удаленному рабочему столу*
Разрешения (Permissions)	Позволяет задавать дополнительные разрешения для данного подключения
Удаленное управление (Remote Control)	Указывает, можно ли удаленно управлять сеансом *Подключение к удаленному рабочему столу,* и если так, то должен ли пользователь выдавать разрешение на инициализацию сеанса удаленного управления. Дополнительные параметры позволяют ограничить сеанс удаленного управления только функцией просмотра либо разрешить полную интерактивность с сеансом клиента *Дистанционное управление рабочим столом*
Параметры клиента (Client Settings)	Позволяют перекрыть параметры из конфигурации клиента, изменить глубину цвета и отключить различные коммуникационные порты (порты ввода-вывода)
Сетевой адаптер (Network Adapters)	Указывает, какие сетевые платы на сервере будут принимать удаленные подключения для администрирования
Общие (General)	Задает уровень шифрования и механизм проверки подлинности для подключений к этому серверу

Устранение неполадок при работе со службами терминалов.

При использовании программы Удаленный рабочий стол для администрирования (Remote Desktop for Administration) создается подключение к консоли сервера. Есть несколько потенциальных причин неудачных подключений или сеансов с ошибками.

• Сбои сети. Ошибки в работе стандартной TCP/IP_сети могут вызывать сбои или разрывы подключений Дистанционное подключение к рабочему столу (Remote Desktop). Если не функционирует служба DNS, клиент не сможет найти сервер по имени. Если не функционирует маршрутизация либо неверно настроен порт Служб терминалов (Terminal Services) (по умолчанию это порт 3389) на клиенте или сервере, соединение установить не удастся.

• Реквизиты входа. Для успешного подключения к серверу средствами программы

Удаленный рабочий стол для администрирования пользователи должны быть включены в группу Администраторы (Administrators) или Пользователи удаленного рабочего стола (Remote Desktop Users). Подготовка к экзамену Если подключиться через Удаленный рабочий стол для администрирования не удается из_за запрета доступа, проанализируйте членство в группах. В предыдущих версиях Сервера терминалов (Terminal Server) для подключения к серверу требовалось быть участником группы Администраторы (Administrators), хотя специальные разрешения можно было выдать вручную. Сервер терминалов поддерживает только два удаленных подключения.

• Политика. Только администраторам разрешено подключаться средствами программы Дистанционное подключение к рабочему столу (Remote Desktop) к контроллерам доменов. Чтобы разрешить подключаться остальным пользователям, нужно настроить политику безопасности на контроллере домена.

• Слишком много параллельных подключений. Если сеансы прерывались без выхода из системы, сервер может посчитать, что достигнут предел, одновременно обрабатываемых подключений, даже если в данный момент к серверу не подключены два пользователя.

Например, администратор может завершить сеанс без выхода из системы. Если еще два администратора попытаются подключиться к серверу, это удастся только одному из них.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

2. Запишите в тетрадь для лабораторных работ основные команды для работы с протоколом TCP/IP;

3. Выполните задания. На этой лабораторной работе вы настроите на сервере Server01 подключения через Удаленный рабочий стол для администрирования (Remote Desktop for Administration). Затем вы оптимизируете Server01, чтобы обеспечить доступность неиспользуемого подключения и разрешить лишь одно подключение в любой момент времени. После этого вы установите сеанс удаленного администрирования с ПК 2 (либо с другого удаленного компьютера).

Если в вашем распоряжении только один компьютер, можно использовать клиент программы Дистанционное подключение к рабочему столу (Remote Desktop) для подключения к службам терминалов на том же компьютере. В этом случае ссылки на удаленный компьютер на этой лабораторной работе будут относится к локальному компьютеру.

Упражнение 1. Настройка удаленного подключения к рабочему столу

В этом упражнении вы активируете удаленное подключение к рабочему столу, измените число разрешенных одновременных подключений на сервере и настроите параметры завершения подключения.

1. Войдите на Server01 как Администратор (Administrator).

2. В Панели управления выберите Система (System Properties).

3. На вкладке Remote включите Remote Desktop. Закройте окно Система (System Properties).

4. Откройте консоль Настройка служб терминалов (Terminal Services Configuration) из группы программ Администрирование (Administrative Tools).

5. В консоли tscc (Terminal Services Configuration\Connections) на правой панели щелкните
правой кнопкой подключение RDP_tcp и выберите Свойства (Properties).

6. На вкладке Сетевой адаптер (Network Adapter) установите значение параметра Максимальное число подключений (Maximum Connections) равным 1.

7. На вкладке Сеансы (Sessions) установите оба флажка Заменить параметры пользователя (Override User Settings) и измените настройки следующим образом: все прерванные любыми способами (или по любой причине) сеансы пользователей закрываются через 15 минут, активный сеанс не ограничивается по времени, сеансы завершаются после 15 минут бездействия.

• Завершение отключенного сеанса (End a disconnected session): 15 минут,

• Ограничение активного сеанса (Active session limit): никогда (never),

• Ограничение активного сеанса (Active session limit): 15 минут.

• При превышении ограничений или разрыве подключения (When session limit is reached or connection is broken): Отключить сеанс (Disconnect from session).

Такая конфигурация обеспечивает следующее: только один пользователь одновременно подключен к серверу терминалов, любой прерванный сеанс закроется через 15 минут и неактивный сеанс прервется через 15 минут. Эти параметры позволяют избежать ситуации, когда прерванный или бездействующий сеанс мешает подключаться средствами программы Удаленный рабочий стол для администрирования (Remote Desktop for Administration).

Упражнение 2. Подключение к серверу с помощью клиента удаленного подключения к рабочему столу

1. На ПК 2 (или на другом удаленном компьютере либо прямо с ServerOl, если удаленного компьютера нет) в группе Стандартные\Связь (Accessories\Communications) щелкните Подключение к удаленному рабочему столу (Remote Desktop Connection), подключитесь к Server01 и войдите в его систему.

2. На сервере Server01 откройте консоль tscc.msc: Администрирование (Administrative tools)\Настройка служб терминалов (Terminal Services Configuration). В открывшейся консоли выберите Подключения (Connections). Вы должны увидеть сведения о сеансе удаленного подключения к Server01.

3. Не выполняйте никаких действий в этом сеансе 15 минут либо закройте клиент программы Удаленное подключение к рабочему столу (Remote Desktop), не завершив сеанс Сервера терминалов (Terminal Server) явно: сеанс должен будет завершиться автоматически через 15 минут.

В данный момент вы подключены к ServerOl удаленно и можете выполнять на нем любые задачи, допустимые в интерактивном режиме на консоли.

Контрольные вопросы

1. Сколько одновременных подключений разрешено к серверу терминалов, работающему в режиме удаленного администрирования? Почему?

2. Как оптимальным образом предоставить администраторам возможность удаленного управления сервером через службы терминалов?

a. Не выполнять никаких действий; они уже имеют доступ, поскольку являются администраторами.

b. Удалить группу Администраторы (Administrators) из списка разрешений в подключении к серверу терминалов и поместить их административную учетную запись в группу Удаленный рабочий стол для администрирования (Remote Desktop for Administration).

c. Создать отдельную пользовательскую учетную запись с более низким уровнем авторизации для повседневного использования группой Администраторы и поместить ее в группу Удаленный рабочий стол для администрирования.

3. Какое программное средство используется на сервере для включения удаленного подключения к рабочему столу?

a. Диспетчер служб терминалов (Terminal Services Manager).

b. Настройка служб терминалов (Terminal Services Configuration).

c. Система (System Properties) из Панели управления.

d. Лицензирование служб терминалов (Terminal Services Licensing).

Сделайте выводы.

Практическое занятие № 7-8

Тема: Установка и настройка системы корпоративной защиты от внутренних угроз.

Цель: получение знаний о методах защиты информации, которым подвергаются компьютерные системы и потерях. Изучение основных понятий и определений, используемых при изучении дисциплины.

Теоретическая часть:

Корпоративная защита от внутренних угроз информационной безопасности

В наши дни одним из наиболее актуальных вопросов защиты корпоративной информации – обеспечение безопасности от внутренних утечек по техническим каналам связи. Одна из главных угроз корпоративной информационной безопасности – неправомерными действиями сотрудников (т.н. инсайдеров), приводящие к потере конфиденциальных данных, совершенные как целенаправленно, так и из-за халатности, невнимательности или незнания элементарных правил безопасности предприятия. Именно «на их совести» большинство громких краж данных, зафиксированных по всему миру в последние годы.

Причиной утечек также могут быть действия посторонних лиц, находящихся на территории предприятия и имеющих доступ к вычислительно сетевой инфраструктуре (клиенты, поставщики и т.п.). Утечки информации могут породить целый ряд проблем:

1. Утечка персональных данных. Может повлечь за собой как санкции со стороны контролирующих органов, так и отток клиентов, связанный с утратой доверия к компании.

2. Утечка коммерческой тайны и ноу-хау. Утечка информации об инвестиционных планах, маркетинговых программах, инновациях, данных клиентской базы способна привести к срыву важных и прибыльных проектов.

3. Утечка служебной переписки. Служебная переписка может дать конкурентам много информации о ситуации в компании. Copyright

4. Утечки в прессу. Могут повлечь за собой разглашение коммерческой тайны организации.

5. Утечка информации о системе безопасности. Открывает широкие возможности для деятельности криминальных структур.

6. Утечка сведений, составляющих государственную тайну и т.д. Необходимость защиты от внутренних и внешних угроз информационной безопасности не только доказана на практике, но и упомянута в ключевых международных стандартах по организации и менеджменту информационной безопасности (например, в ISO/IEC 27001).

Технологии корпоративной защиты от внутренних угроз информационной безопасности, относящиеся к классу Data Leak Prevention (DLP) позволяют выявлять и предотвращать утечки конфиденциальной информации и персональных данных, защищать компании от мошенничества, воровства и коррупции, детектировать неправомерные действия сотрудников и нецелевое использование корпоративных ресурсов. Системы корпоративной безопасности позволяют однозначно выявлять инциденты и дают весь необходимый набор инструментов для проведения внутренних расследований и дальнейшей правовой защиты корпоративных интересов.

Специалисты по корпоративной безопасности должны обладать теоретическими знаниями по обеспечению корпоративной защиты от внутренних угроз, понимать аспекты применения нормативно-правовой базы для классификации и расследования инцидентов, в совершенстве владеть системами и технологиями для достижения целей защиты.

Неотъемлемой частью работ по обеспечению корпоративной безопасности от внутренних утечек является проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его. Для этого специалисты должны уметь проводить весь цикл работ по установке, развёртыванию, настройке, использованию DLP систем, включая разработку политик информационной безопасности, классификацию объектов защиты, применение технологий фильтрации различных видов трафика, фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.

Важным направлением обеспечения безопасности корпоративной информации – реализация прозрачного доступа к территориальнораспределенным информационным ресурсам компании через сети связи общего пользования, в том числе Интернет. Для защиты передаваемых данных используется технологии виртуальной частной сети (Virtual Private Network, VPN) и межсетевого экранирования, включая:

• защиту информации, передаваемой по каналам связи;

• защиту сети в целом, ее сегментов от несанкционированного доступа, как из внешних, так и из внутренних сетей;

• контроль трафика между узлами VPN-сети, включая фильтрацию трафика;

• использование в качестве транспортной среды передачи данных каналы сетей связи общего пользования;

• возможность модернизации, модульного наращивания VPN-сети;

• централизованное управление VPN-сетью. Для предотвращения и минимизации последствий атак на корпоративную инфраструктуру и объекты защиты, необходимо их своевременное выявление и правильная классификация с использованием технологий класса IDS (Intrusion Detection System).

Помимо перечисленного, специалист по корпоративной безопасности должен уметь подготовить отчёты о найденных инцидентах (с оценкой уровня угрозы и нормативной оценкой) менеджменту организации, которую защищает, а также правильно оценить угрозы и риски информационной безопасности.

Корпоративные и экономические интересы

Понятие «корпоративная безопасность» в последние годы несколько изменилось по сравнению с 90-ми годами. Тогда внимание акцентировалось на личной безопасности собственника бизнеса и имущества. Связано это было с огромной криминализацией в стране, в те времена можно было уберечься от преступности только с помощью физической охраны и технических средств. Тогда и появляется «институт» телохранителей, ведь необходима была защита практически каждому бизнесмену.

Со временем государство начало более и менее заниматься вопросами регулирования экономических процессов в стране, и проблемы безопасности перетекли в плоскость экономики. Тогда практически все предприятия работали с огромными нарушениями, ведь налогообложение было непомерным. В итоге появились множественные схемы, которые позволили уводить деньги в тень. А угрозу стали нести контролирующие органы. В большинстве случаев возврат средств производился силовыми методами. Тогда и появилось понятие экономической безопасности. На предприятиях создавались специальные отделы, сотрудники которых занимались уже не физической охраной, а защищали информацию экономического характера. В итоге уволившиеся сотрудники правоохранительных органов стали устраиваться в такие отделы либо организовывать свои предприятия, оказывающие услуги по экономической безопасности. Хотя фактически они напоминали структуры МВД и ФСБ, которые попросту решали вопросы своих работодателей.

Последние годы эта практика уходит в небытие. Но развитие рыночных отношений порождает новые проблемы. Теперь перед бизнесменом стоят новые задачи. Теперь свое «детище» необходимо защищать от поглощения, происков конкурентов. А это угроза не только собственнику, но и экономической стабильности всей страны (монополизация отдельных отраслей, безработица и снижение доходности бюджета).

Виды конкуренции

На сегодняшний день выделяют три вида конкуренции:

- «Белая», то есть добросовестная, проводимая открыто и в рамках нормативных документов.
- «Серая», нацеленная на дискредитацию предприятия, с использованием методик, запрещенных действующим законодательством.
- «Черная». Это фактически противоборство, целью которого является уничтожение конкурента.

В свете этой классификации выделяют два вида угрозы: недружественное поглощение и промышленный шпионаж.

Другая угроза безопасности бизнеса – коррупция в контролирующих и проверяющих органах. Недобросовестные сотрудники таких органов вымогают взятки, даже если у предприятия нет нарушений, то есть такая практика считается нормальной. Помимо этого, взяточники могут выступать инструментом в недобросовестной конкуренции.

А криминалитет на сегодняшний день уходит на последний план, угроза от организованной преступности фактически осталась в прошлом.

Существует и так называемая целенаправленная угроза, то есть когда сотрудники предприятия совершают заведомо неправильные действия, которые несут

непосредственную угрозу бизнесу. Это может быть также кража или взлом компьютерной системы, продажа секретной информации.

С чего начать?

Система корпоративной безопасности должна начинаться с определения круга угроз - как временных, так и постоянных, и в целом состоит из нескольких подсистем, а именно:

- защиты информации;
- кадровой безопасности;
- технической;
- юридической; экономической и других.

Начать рекомендуется с выбора лица, которое будет ответственным за систему безопасности, либо создания отдела. Помимо этого, можно привлечь специализированную компанию на условиях аутсорсинга.

Уже человек, который будет заниматься непосредственно построением системы, обязан определить степень обеспечения сохранности информации и доступ к ней. Затем определяются методы защиты информационных ресурсов, которые подразделяются на открытые и закрытые.

Работа с персоналом

Понятие экономической безопасности включает в себя не только кражи на уровне низшего состава, к примеру, кражу каких-то запасных частей или бумаги, но и халатность со стороны работников. Бывают случаи, что сотрудники совершают проступки по простому незнанию или халатности, передают конфиденциальные сведения о предприятии, где они работают, третьей стороне или конкурентам.

Поэтому очень важно, чтобы на предприятии о корпоративной безопасности знали все сотрудники, и не только знали, но и понимали степень персональной ответственности. Это касается даже открытия фишинговых писем, которые в действительности могут нести потенциальную угрозу всему предприятию. Халатность может проявляться даже в том, что работник может переслать важное письмо не по тому адресу.

Другие случаи утечки информации

Следует понимать, что корпоративная информационная безопасность должна касаться не только рядовых сотрудников. Как показывает практика, даже среди учредителей встречаются так называемые «крысы». Такие люди, как правило, имеют свободный доступ к любой информации, но другие совладельцы совершенно не застрахованы от того, что один из них ведет двойную игру и является инсайдером.

Среди инсайдеров выделяют и среднее звено руководителей, топ-менеджеров. Эти люди также способны действовать в корыстных целях, но и попросту могут халатно относиться к безопасности. Но все же чаще всего ведут двойную игру, пользуются своими привилегиями и злоупотребляют доступом к конфиденциальной информации организации наемные руководители.

И, как говорилось ранее, красть ценную информацию могут обычные, рядовые сотрудники с целью получения наживы за ее разглашение. Но это случается достаточно редко, чаще всего утечка происходит на фоне халатности и неосторожности. Хотя наверняка многие предприниматели сталкивались с ситуацией, когда ушедший сотрудник устраивается к конкурентам и переманивает всех клиентов, которых наработала компания, то есть фактически ворует базу клиентов.

Базовые методы защиты

Что может сделать отдел экономической безопасности? Прежде всего на предприятии должен быть организован контролируемый доступ на территорию. Не важно будет ли это физический контроль либо специальное программное обеспечение с выдачей карты, главное, чтобы система работала, и на территорию был ограничен доступ посторонних лиц.

Во-вторых, если на предприятии множество подразделений, то можно организовать систему с доступом в конкретные отделы с HID-картами. Проще говоря, зайти в конкретное подразделение сможет лишь тот человек, который имеет разрешение.

Защита информации

Корпоративная безопасность в части защиты информации, которая хранится на виртуальных носителях, состоит из следующих мер:

- установка программного обеспечения, которое будет контролировать передачу данных с каждого компьютера предприятия;
- блокировка BIOS, с целью предотвращения внесения любых изменений в систему;
- отключение оптических приводов;
- отказ от пиратских версий офисных программ и использование только лицензионного программного обеспечения.

На сегодняшний день существует множество программ, позволяющих отследить действия сотрудников на компьютерах. В частности, программы позволяют даже определить дату прихода и ухода сотрудника, период отсутствия на рабочем месте. И самое главное, на какие сайты осуществлялись переходы с конкретного рабочего места, какая просматривалась информация и в каких программах работал сотрудник.

Безопасность корпоративных сетей состоит также в установке антивирусных программ, систем, которые позволят отфильтровать нежелательную почту и удалить ее из корпоративного почтового ящика.

Не стоит забывать и об организации дифференциального доступа, а также системной смене паролей. Рекомендуется также организовать систему, которая позволит делать резервное копирование файлов. То есть информация не должна храниться исключительно на компьютерах, она должна дублироваться на сервере или другом внешнем носителе. Такие мероприятия позволяют защитить данные не только от кражи, но и от непредвиденных ситуаций, к примеру, в случае изъятия компьютерной техники правоохранительными органами.

Корпоративная связь в интернете должна осуществляться в зашифрованном виде, рекомендуется использовать протокол end-to-end protection. Этот формат и другие шифрования позволяют подтвердить подлинность передаваемого документа и защитить информацию, содержащуюся в нем.

Защита от недружественного поглощения

В обязанности сотрудников отдела экономической безопасности также должна входить защита от поглощения. В частности, сотрудники подразделения обязаны:

- Отслеживать приобретение акций компании. Если речь идет об ОАО, то беспокойство должна вызывать скупка большого количества акций, для ЗАО и ООО даже 1 акция имеет огромное значение.
- Мониторинг внутреннего рынка. Поглощение может быть не только из-за того, что с рынка хотят убрать определенную компанию, но и на фоне того, что у предприятия может быть привлекательная недвижимость или другое ценное имущество.
- Контролировать немотивированные запросы документов. Они могут поступать по корпоративной связи, почте, через интернет. Но важно не это – опасно, если

обращается за информацией миноритарный акционер. Вызвать подозрение должен и запрос от акционера, у которого 1 или 2 акции, и он даже не принимает участие в голосовании. Отслеживать необходимо немотивированные запросы от контролирующих и правоохранительных органов, так как через таких сотрудников могут действовать недружественные компании.

- Тщательный контроль кредиторской задолженности. Нередки случаи, когда захват активов происходил именно из-за аккумулирования долгов в одних руках.

Практическое задание:

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.

Средства комплексной защиты от потенциальных угроз.

Обеспечение качества в системе безопасности.

Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

Правовое обеспечение юридических отношений с работниками Предприятия .

Правовое обеспечение юридических отношений с партнерами Предприятия.

Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

Практическое занятие № 9-10

Тема: Запуск системы, проверка функциональности и соответствия настроек целевой сетевой инфраструктуре.

Цель: организовать автоматизированную систему управления IT-инфраструктурой корпоративной сети в учебных целях — получить практические навыки в централизованном управлении, используя платформенный подход.

Теоретическая часть:

Логические уровни сетевой инфраструктуры

Использование ОССН в составе АСЗИ подразумевает организацию сетевого взаимодействия компьютеров, функционирующих под её управлением в составе ЗЛВС.

АСЗИ – это автоматизированная система в защищенном исполнении

ЗЛВС — защищённая локальная вычислительная сеть.

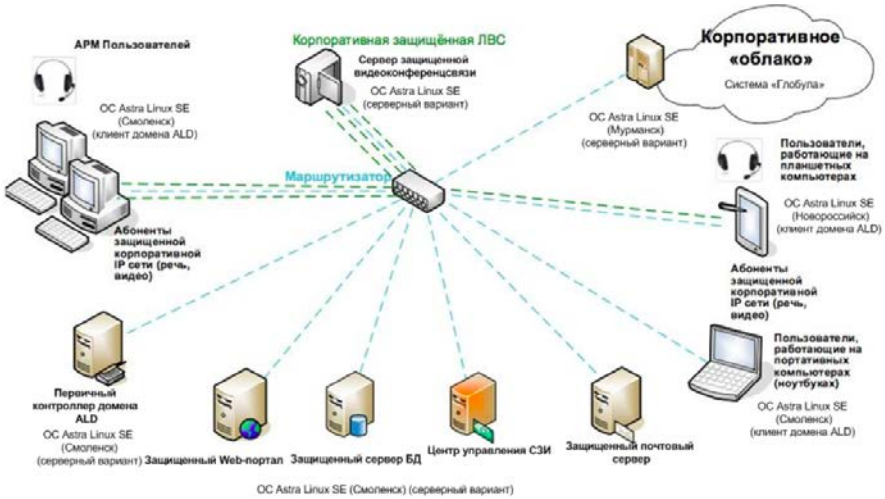


Рисунок 1. Вариант реализации корпоративной ЗЛВС для мультисервисной системы связи на базе ОССН Astra Linux Special Edition (релизы Смоленск, Мурманск, Новороссийск).

Поскольку в качестве базового стека сетевых протоколов в ОССН используется стек TCP/IP, методика создания подобных ЗЛВС основана на методике создания сетевой инфраструктуры на базе этого стека протоколов. При этом организация сетевой инфраструктуры может рассматриваться, как минимум, на двух логических уровнях:

- базовом, подразумевающем организацию сетевого взаимодействия компьютеров (хостов), работающих под управлением ОССН в составе одной или нескольких подсетей со статическим или динамическим выделением IP-адресов, реализацией статической маршрутизации между хостами, входящими в разные подсети, а также организацией шлюза для доступа в сеть Интернет;
- корпоративном, подразумевающем организацию доменной сетевой инфраструктуры на базе варианта службы каталогов (Directory Service), обеспечивающей её пользователям механизм ЕПП (Единое пространство пользователей), включая централизованное управление учётными записями пользователей и групп пользователей, прозрачную (сквозную) аутентификацию в ЕПП с любого хоста, являющегося клиентом домена и централизованное хранение домашних каталогов пользователей.

В этом случае модули LSM Module Policy Engine подсистемы безопасности ОССН PARSEC раздельно реализуют управление доступом (hooks/decision) для каждого из указанных логических уровней:

- LSM-модуль parsec обеспечивает управление доступом на уровне стека протоколов TCP/IP (реализован для версии протокола IPv4);
- LSM-модуль parsec-cifs обеспечивает управление доступом на уровне протокола прикладного уровня CIFS — диалекта протокола SMB (реализован для версии протокола SMB 3.0).

Linux Security Modules (LSM) — фреймворк, добавляющий в Linux поддержку различных моделей безопасности. LSM является частью ядра начиная с Linux версии 2.6. На данный момент в официальном ядре «обитают» модули безопасности SELinux, AppArmor, Tomoyo и Smack.

Работают модули параллельно с «родной» моделью безопасности Linux — избирательным управлением доступом (Discretionary Access Control, DAC). Проверки LSM вызываются на действия, разрешенные DAC.

Применять механизм LSM можно по-разному. В большинстве случаев это добавление мандатного управления доступом (как, например, в случае с SELinux). Кроме того, можно придумать собственную модель безопасности, реализовать ее в виде модуля и легко внедрить, используя фреймворк.

SMB (сокр. от англ. Server Message Block) — сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия. Первая версия протокола, также известная как Common Internet File System (CIFS) (Единая файловая система Интернета), была разработана компаниями IBM, Microsoft, Intel и 3Com в 1980-х годах; вторая (SMB 2.0) была создана Microsoft и появилась в Windows Vista. В настоящее время SMB связан главным образом с операционными системами Microsoft Windows, где используется для реализации «Сети Microsoft Windows» (англ. Microsoft Windows Network) и «Совместного использования файлов и принтеров» (англ. File and Printer Sharing). В Windows Server 2012 используется новая версия протокола SMB — SMB 3.0.

Очевидно, что корпоративный уровень сетевой инфраструктуры может быть развернут только поверх базового уровня.

Формирование базового уровня сетевой инфраструктуры ОССН

В общем случае процесс создания базового уровня сетевой инфраструктуры ОССН состоит из этапов, приведенных на рис. 2.

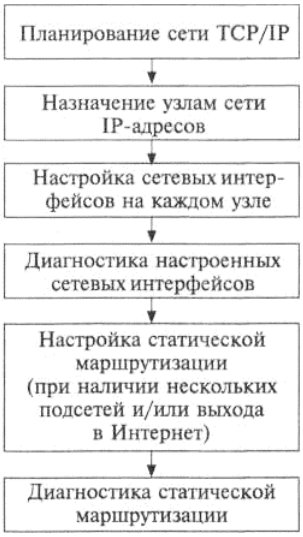


Рисунок 2. Этапы формирования базового уровня сетевой инфраструктуры ОССН.

В ОССН указанные этапы реализуются с помощью ряда средств, стандартных для большинства современных дистрибутивов ОС проекта GNU/Linux, к ним относятся:

- net tools — набор команд конфигурирования сетевой инфраструктуры на базе стека TCP/IP;
- iproute2 — альтернативный набор команд конфигурирования сетевой инфраструктуры на базе стека TCP/IP, учитывающий такие его особенности, как туннелированние сетевых протоколов, возможность формирования виртуальных частных сетей (VPN) и средства управления трафиком (качеством обслуживания);
- графические утилиты, встроенные в защищённую графическую подсистему Fly.

Далее будут рассматриваться команды из набора net tools поскольку именно он рекмендуется в документации на ОССН в качестве основного средства администрирования базовой сетевой инфраструктуры. В текущий версии ОССН в набор net tools входят команды, указанные в табл. 1. Для создания базовой сетевой инфраструктуры основными из представленных в табл. 1 являются команды ifconfig, netstat, arp и route.

Настройка сетевых интерфейсов. Для настройки сетевых интерфейсов используется команда ifconfig (от Interface Configuration), выполняющая следующие функции:

- назначение IP-адреса;
- назначение широковещательного адреса и связанной с ним маски подсети;
- включение (up) и выключения (down) сетевого интерфейса.

```
test@astra:~$ sudo ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e0:38:63
          inet addr:192.168.100.105  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:502 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3774829 (3.5 MiB)  TX bytes:57049 (55.7 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1100 (1.0 KiB)  TX bytes:1100 (1.0 KiB)
```

Обычно команда ifconfig применяется во время первоначальной настройки сети, но может использоваться и для внесения изменений в ходе её эксплуатации. Пример вывода этой команды приведён на рис. 3.

Рисунок. 3. Пример вывода команды ifconfig

Управлять конфигурированием сетевых интерфейсов администратор ОССН может не только с помощью команды ifconfig, но и с использованием графической утилиты «Сетевые соединения» (вызываемой из главного пользовательского меню через меню «Настройки»), предназначенной для настройки параметров проводных и беспроводных сетевых интерфейсов.

Доступ к графической утилите «Сетевые соединения» можно получить из области уведомлений рабочего стола Fly (рис. 4).

Рисунок 4. Доступ к графической утилите «Сетевые соединения» из области уведомлений рабочего стола Fly

В основном окне интерфейса графической утилиты «Сетевые соединения» отображаются обнаруженные автоматически сетевые интерфейсы, при этом предоставляются возможности:

- отключить/включить сетевой интерфейс;
- вызвать интерфейс настроек IP-адресации (рис. 5,6);

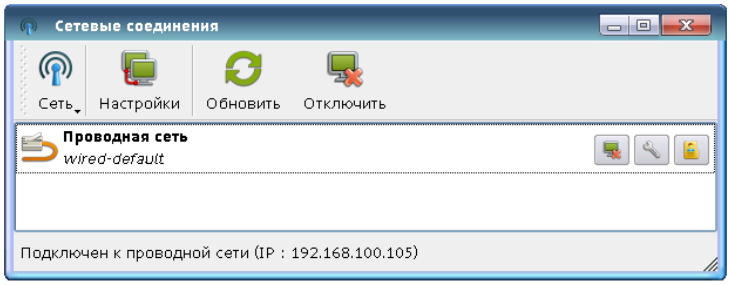


Рисунок 5. Окно «Сетевые соединения». Для вызова окна «Настройки нужно щелкнуть кнопкой мыши по опции «Настройки».

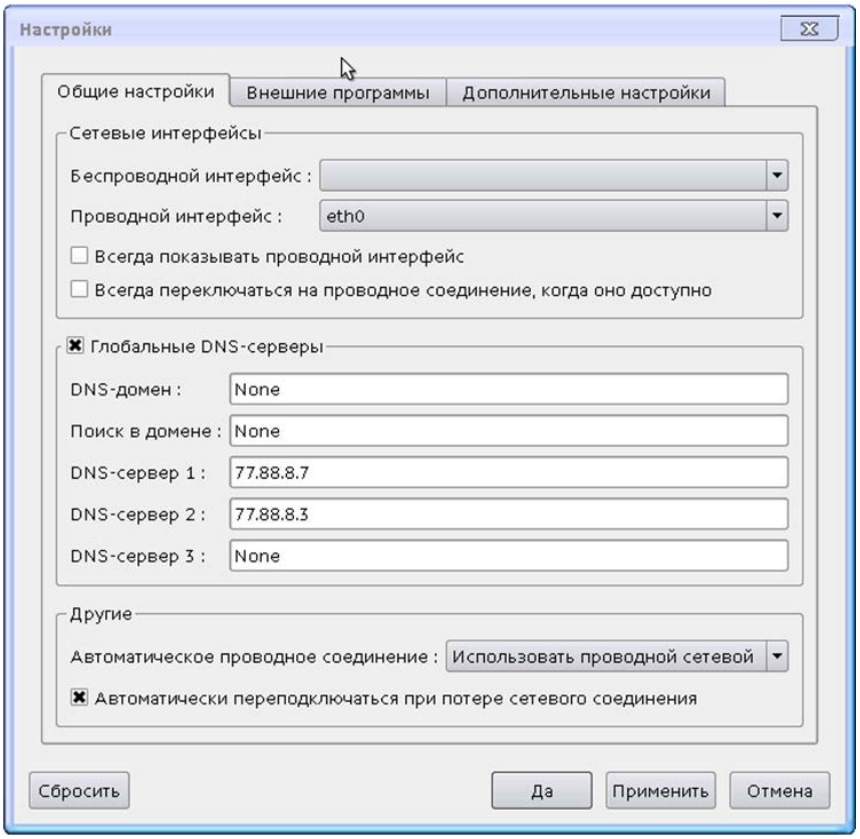
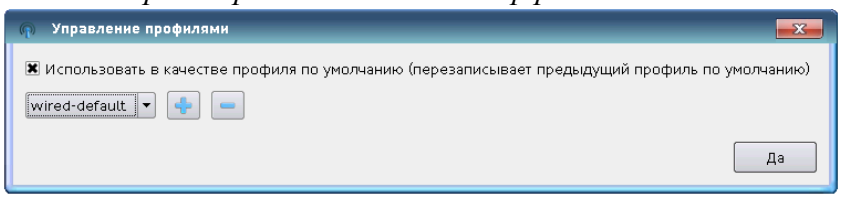


Рисунок 6. Управление параметрами сетевого интерфейса.



- задать сетевой интерфейс в сетевом профиле по умолчанию (default) (рис. 7);

Рис. 7. Управление профилями сетевого интерфейса

- осуществить настройки сетевого интерфейса (рис. 6)

При успешном конфигурировании адресной информации сетевого интерфейса в области уведомлений рабочего стола Fly появится соответствующее *сообщение об успешном сетевом подключении (рис. 8).*

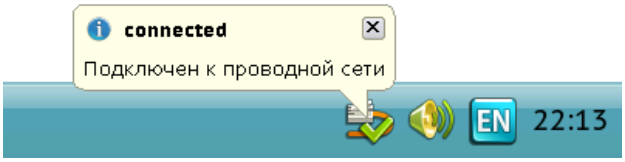


Рисунок 8. Уведомление об успешном подключении сетевого интерфейса.

При этом следует учитывать, что поскольку ОССН адаптирована для работы с мобильными устройствами (планшетными компьютерами), в разделе «Сетевые интерфейсы» и во вкладке «Дополнительные настройки» графической утилиты «Сетевые соединения» предоставлены функции конфигурирования беспроводных сетевых интерфейсов и правила переключения между проводным и беспроводным интерфейсами.

Проверка и настройка базового уровня сетевой инфраструктуры. Команда netstat отображает информацию о состоянии сетевого ПО, включая статистику сетевых интерфейсов и данные из таблицы маршрутизации. Наиболее востребованными её функциями являются:

- вывод информации о конфигурации и статистике работы сетевых интерфейсов;
- получение статических данных о сетевых протоколах;
- проверка состояния сетевых соединений;
- просмотр таблицы маршрутизации.

Команда arp используется для просмотра, добавления и удаления записей в специальной системной таблице ядра ОССН — кэше ARP, в которой задано соответствие IP-адресов хостов сети аппаратным интерфейсам сетевых адаптеров (Аппаратным (MAC) адресам).

MAC-адрес или HW-адрес (от англ. Media Access Control — управление доступом к среде, также Hardware Address) — уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.

При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь уникальный шестибайтный номер (MAC-адрес), «прошитый» в ней при изготовлении. Этот номер используется для идентификации отправителя и получателя фрейма; и предполагается, что при появлении в сети нового компьютера (или другого устройства, способного работать в сети) сетевому администратору не придётся настраивать этому компьютеру MAC-адрес вручную.

Уникальность MAC-адресов достигается тем, что каждый производитель получает в координирующем комитете IEEE Registration Authority диапазон из шестнадцати миллионов адресов и, по мере исчерпания выделенных адресов, может запросить новый диапазон. Поэтому по трём старшим байтам MAC-адреса можно определить производителя.

Для интерфейсов сети Ethernet в кэше ARP устанавливается соответствие между IP-адресом хоста и MAC-адресом его сетевого адаптера. Для опроса хостов на предмет этой информации используется специальный протокол сетевого уровня ARP. Он передаёт широковещательные пакеты, которые не могут выйти за пределы локальной сети, т. е. протокол ARP позволяет находить только адреса хостов, работающих в пределах одной сети (подсети). Рассылка пакетов протокола ARP происходит вскоре после начальной загрузки ОССН, поэтому протокол ARP практически не влияет на загруженность сети.

```
test@astra:~$ cat /proc/self/net/arp
IP address       HW type     Flags       HW address            Mask     Device
192.168.100.5    0x1         0x2         00:15:5d:64:70:03     *        eth0
192.168.100.15   0x1         0x2         00:15:5d:64:70:04     *        eth0
192.168.100.107  0x1         0x2         00:1c:c0:30:0a:5a     *        eth0
192.168.100.3    0x1         0x2         00:15:5d:64:70:05     *        eth0
192.168.100.1    0x1         0x2         e4:8d:8c:dd:d4:41     *        eth0
192.168.100.100  0x1         0x2         00:80:f0:1d:37:1e     *        eth0
```

Маршрутизация в ОС семейства Linux может использоваться следующих двух видов:

- статическая маршрутизация — когда маршруты задаются явно и хранятся в таблице маршрутизации до момента необходимости их удаления;
- динамическая маршрутизация — выполняющаяся демонами routed или gated, которые заполняют и модифицируют таблицу Kernel IP routing table на основе сообщений от других хостов сети (динамическая маршрутизация необходима в том случае, если структура сети не является статичной и меняется с течением времени, и в ней один и тот же компьютер может быть доступен по различным интерфейсам, например, через разные адаптеры Ethernet или беспроводный интерфейс).

```
test@astra:/proc$ sudo route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.100.1   0.0.0.0         UG    0      0        0 eth0
192.168.100.0   *               255.255.255.0   U     0      0        0 eth0
```

Рисунок. 11. Пример вывода таблицы Kernel IP routing table командой route

Поскольку в состав дистрибутива ОССН не включены демоны routed и gated, динамическая маршрутизация в ней не реализуется.

В случае использования на хосте двух и более сетевых интерфейсов (например, когда хост применяется в качестве маршрутизатора или шлюза в другую подсеть) требуется указать ядру ОССН на необходимость включения функции «IP forwarding», которая позволяет перенаправлять IP-пакеты с одного сетевого интерфейса на другой. Это осуществляется путём вызова команды sysctl. Для того чтобы функция «IP forwarding» применялась каждый раз при загрузке/перезагрузке ОССН, необходимо задать соответствующий параметр в конфигурационном файле /etc/sysctl.conf (рис. 12).

```
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Рисунок 12. Строка включения функции «IP forwarding» для протокола IPv4

Практическое задание:

В процессе занятия решаются следующие задачи:

1. познакомить с основными принципами работы текстовых протоколов;
2. научить учащихся основным способам работы с прикладным протоколом Telnet;

Краткие теоретические и справочно-информационные материалы по теме занятия. Большинство протоколов высших уровней – текстовые – запросы и ответы передаются в виде текста, т.е. в запросах и ответах могут присутствовать только печатные символы.

Во многих протоколах ответы начинаются со специальной строки, состоящей из трехзначного числа и, возможно, текстового описания типа ответа. Трехзначное число

разделяется на две части: 1-ый символ рассматривается как код класса сообщения; два последние – как тип сообщения данной важности.

Коды классов следующие:

1 – информационное сообщение. Обычно игнорируется программными клиентами.

2 – удачное завершение запроса. Рассматривается программами-клиентами как успех обработки запроса и обычно игнорируется.

Часто программы-серверы не различают сообщения первого и второго типа, т.е. информационное сообщение проходит по второй категории.

3 – сообщение об удачной обработке запроса, но требующее дополнительных действий клиента.

4 – ошибка со стороны клиента, т.е. клиент послал запрос, который не может обработать сервер вследствие ошибочности или недостаточности данных.

5 – ошибка со стороны сервера. Клиент послал правильный запрос, но сервер не смог
его выполнить в силу каких-то причин.

Трехзначные коды ответов очень удобны для программного распознавания, нет необходимости распознавать текст ответа, который, в общем случае, может прийти на разных языках, достаточно распознать только 3 цифры.

2. Программа TELNET

Для работы с текстовыми протоколами воспользуемся программой TELNET, входящей в состав Windows. Эта программа предназначена для работы с протоколом TELNET, задачей которого является обмен информацией между клиентом и сервером без каких либо преобразований, т.е. организация прозрачного канала между клиентом и сервером.

Синтаксис команды TELNET следующий:

TELNET адрес_сервера [порт]

Если порт не указан, используется 23 - стандартный порт протокола TELNET.

3. Протокол SMTP

Для начала попробуем поработать с протоколом SMTP. Обычно он работает, используяпорт 25.

Для наглядности команды пользователя выделены курсивом, а ответы сервера – подчеркиванием.

Даем команду на подключение:

telnet 192.168.1.2 25

Получаем ответ

220 home VPOP3 SMTP Server Ready

Работает! Обратите внимание на число 220 в начале строки ответа. Это нормальный ответ, сервер ответил на наш запрос на подключение.

Многие серверы, работающие по текстовым протоколам, поддерживают команду HELP. Проверим.

Help

Дадим серверу неправильный запрос

abrakadabra

500 Command Unrecognised

Как ни странно, но код ответа 5 – ошибка на стороне сервера!

Попробуем написать письмо

Поздороваемся

helo home

250 home VPOP3 SMTP Server - Hello home, pleased to meet you

Укажем отправителя письма

mail from: user1

250 <user1>... Sender ok

Укажем получателя письма

rcpt to: user2

250 <user2>... Recipient ok

Перейдем в режим ввода письма

data

354 Start Mail input, end with <CRLF>.<CRLF>

Обратите внимание на код ответа 354.

Это нормальное завершение, но требуются дополнительные данные – само письмо, которое, как видно, должно заканчиваться строкой, состоящей из одной точки «.».

А теперь само письмо. Формат письма описан стандартами. Их изучение не входит внашу задачу, но наиболее важные служебные строки вкратце рассмотрим:

Date: Tue, 22 Nov 2005 19:55:07 +0200

Дата создания по GMT и часовой пояс

From: User user1@home.my

От кого

Reply-To: User user1@home.my

Кому отвечать

To: user2@home.my

Кому

Subject: Test

Тема письма

MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

Информация почтовой программе, как закодировано письмо – с помощью этих строк

почтовая программа клиент сможет реализовать шестой уровень – представить информацию пользователю в читабельном виде

Hello user2,

It's a test message.

Best regards,

User mailto:user1@home.my

Само письмо

.250 OK

Письмо принято!

Теперь выходим

quit

221 home VPOP3 Server Closing Connection

Протокол SMTP (Simple Mail Transfer Protocol) используется для передачи электронной почты от клиента серверу или между серверами. Не содержит встроенных средств идентификации и преобразования.

4. Протокол POP3

Теперь поработаем с протоколом POP3. Обычно он работает, используя порт 110.

Даем команду на подключение:

telnet 192.168.1.2 25

Получаем ответ

+OK VPOP3 Server Ready <1.7b0.435a37>

Работает, но трехсимвольного кода ответа нет!

Попробуем help

help

-ERR Unrecognised command

Видим, что помощи нет, заодно и посмотрели, как сервер отвечает на ошибочный для

него запрос.

Как мы знаем, POP3 требует аутентификации, поэтому представимся:

user user2

+OK User Accepted, PASSword required

А теперь пароль.

pass 2

+OK user2 has 1 message(s) (580 octets)

Нам есть почта! Посмотрим.

list

+OK 1 messages (580 octets)

1 580

.

Одно письмо 580 символов. Если бы было несколько писем, было бы несколько строк с

указанием номеров и размеров писем. Точка в последней строке показывает, что это окончание ответа.

Теперь прочитаем (получим) первое письмо.

retr 1

+OK 580 octets

Received: from 192.168.200.1 by home ([192.168.200.1] running VPOP3) with SMTP

or <user2>; Tue, 22 Nov 2005 20:31:07 +0200

Date: Tue, 22 Nov 2005 19:55:07 +0200

From: User <user1@home.my>

Reply-To: User <user1@home.my>

To: user2@home.my

Subject: Test

MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

Message-Id: <VPOP31.3.0c.20051122203134.814.e.1.40132205@home>

X-Server: VPOP3 V1.3.0c - Registered to: Collega

Hello user2,

It's a test message.

Best regards,

User mailto:user1@home.my.

Служебных полей стало больше – их добавил сервер.

Обратите внимание на последнюю строку ответа

Теперь удалим письмо с сервера, ведь оно уже прочитано:

dele 1

+OK message 1 deleted

Проверим, есть ли что еще

list

+OK 0 messages (0 octets).

Ничего нет. А можно и так, для программы это будет более удобным

list 1

-ERR Invalid Message Number

Ну, и теперь выходим

quit

+OK VPOP3 Server Closing Connection

В приведенном выше примере было отправлено письмо от пользователя «user1» пользователю «user2» и получена почта пользователя «user2» с помощью утилиты TELNET, т.е. без использования почтового клиента.

Протокол POP3 (Post Office Protocol) предназначен для получения электронной почты от сервера к клиенту. Содержит средства идентификации клиента, использует факультативные средства преобразования.

5. Протокол FTP

Протокол FTP (File Transfer Protocol) – протокол передачи файлов.

Он использует 20-ый порт для установления соединений и 21-ый порт для установления соединений и передачи файлов. Этот протокол содержит встроенные средства идентификации клиента. Все распознаваемые им команды состоят из 3-х или 4-х символов, являющихся сокращениями или аббревиатурами выполняемых действий.

6. Протокол HTTP

Протокол HTTP (Hyper Text Transfer Protocol) – протокол передачи гипертекста, т.е.

данных разного представления (текст, изображения, видео, звук). Обычно этот протокол работает на 80-ом порту. Он содержит средства идентификации и перекодирования передаваемой информации.

Как видим работа с текстовыми протоколами не представляет особых трудностей.

Правда некоторые протоколысодержат большое число команд и чтобы узнать их формат требуется использовать их стандарт и описания RFC.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

2. Запишите в тетрадь для лабораторных работ основные команды для работы с протоколом TCP/IP;

3. Выполните задания

Во всех заданиях адрес сервера:192.168.1.2

В пятом и шестом заданиях, после аутентификации (если она необходима) рекомендуется в первую очередь вызвать помощь командой help и посмотреть информацию о других командах, поддерживаемых данным протоколом.

1. Используйте адрес сервера электронной почты, установленного на VirtualBox (если почтовый сервер не установлен установите его), имена и пароли пользователей. Отправить и получить почту без использования почтового клиента.

2. Поработать с POP3 без аутентификации. Сделать соответствующие выводы.

3. Определить, является ли протокол FTP текст-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.

4. Подключиться к HTTP серверу и определить, является ли протокол HTTP тексториентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.

5. Использовать адрес и порт неизвестного для вас протокола и сервера. Получите список его команд, объясните, что делает каждая команда. Попробовать некоторые из них и проанализировать результаты.(использовать 1000-ый порт, при аутентификации имя пользователя и пароль: admin).

6. Поработайте с FTP-сервером с помощью TELNET и программы FTP. Объясните и подтвердите на конкретном примере разницу между ними. Для запуска программы FTP в командной строке вызвать ftp>open (узел)……)

Практическое занятие № 11-13

Тема: Имитация процесса утечки конфиденциальной информации в системе

Цель: изучить протоколирование и аудит, а также криптографические методы защиты. Показать их место в общей архитектуре безопасности.

Теоретическая часть:

Построение систем защиты от угрозы конфиденциальности. Причины и виды утечки информации

Нарушение конфиденциальности происходит в результате утечки информации. Защита информации от утечки – это деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Основными причинами утечки информации являются:

• несоблюдение персоналом норм, требований, правил эксплуатации АС;
• ошибки в проектировании АС и систем защиты АС;
• ведение противостоящей стороной технической и агентурной разведок.

Несоблюдение персоналом норм, требований, правил эксплуатации АС может быть как умышленным, так и непреднамеренным. От ведения противостоящей стороной агентурной разведки этот случай отличает то, что здесь лицом, совершающим несанкционированные действия, двигают личные побудительные мотивы. Причины утечки информации достаточно тесно связаны с видами утечки информации.

В соответствии с ГОСТ Р 50922–96 рассматриваются три вида утечки информации:

• разглашение;
• несанкционированный доступ к информации;
• получение защищаемой информации разведками (как отечественными, так и иностранными).

Под разглашением информации понимается несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации.

Согласно несанкционированный доступ к информации – доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под НСД понимается получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

При этом заинтересованным субъектом, осуществляющим несанкционированный доступ к информации, может быть государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Получение защищаемой информации разведками может осуществляться с помощью технических средств (техническая разведка) или агентурными методами (агентурная разведка).

Классификация каналов утечки информации

Канал утечки информации – совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может быть в пределах контролируемой зоны, охватывающей АС, или вне ее.

При выявлении каналов утечки информации необходимо рассматривать всю совокупность элементов системы, включающую основное оборудование технических средств обработки информации (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрофикации, радиофикации, часофикации, электробытовые приборы и др.

В качестве каналов утечки большой интерес представляют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещения с установленными в них основными и вспомогательными 65 техническими средствами, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

Следует помнить о внутренних каналах утечки информации, связанных с действиями администрации и обслуживающего персонала, с качеством организации режима работы, тем более что обычно им не придают должного внимания. Из них в первую очередь можно отметить такие каналы утечки, как хищение носителей информации, съем информации с ленты принтера и плохо стертых дискет, использование производственных и технологических отходов, визуальный съем информации с дисплея и принтера, несанкционированное копирование и т. п.

Каналы утечки информации по физическим принципам можно разделить на следующие группы:

• акустические (включая и акустопреобразовательные). Связаны с распространением звуковых волн в воздухе или упругих колебаний в других средах;

• электромагнитные (в том числе магнитные и электрические);

• визуально-оптические (наблюдение, фотографирование). В качестве средства выделения информации в данном случае могут рассматриваться фото-, видеокамеры и т. п.;

• материально-вещественные (бумага, фото, магнитные носители, отходы и т. п.);

• информационные. Связаны с доступом к элементам ТКС, носителям информации, самой вводимой и выводимой информации, к программному обеспечению, а также с подключением к линиям связи.

На практике применяется также деление каналов утечки на технические (к ним относятся акустические, визуально-оптические и электромагнитные) и информационные.

Технические каналы утечки информации

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве излучения, которые в той или иной степени связаны с обрабатываемой информацией (акустическое и электромагнитное излучение, ПЭМИН). Правомерно предполагать, что образованию каналов утечки информации способствуют также определенные обстоятельства и причины технического характера (несовершенство схемных решений, эксплуатационный износ элементов изделия).

В любых технических средствах существуют те или иные физические преобразователи, которые выполняют соответствующие им функции, основанные на определенном физическом принципе действия. Однако помимо 66 основных своих функций такие преобразователи в соответствии со своей физической природой способны порождать и дополнительные каналы утечки.

Знание всех типов физических преобразователей позволяет решать задачу определения возможных неконтролируемых проявлений физических полей, образующих каналы утечки информации.

Особенности акустических каналов утечки информации

Наиболее ценной акустической информацией чаще всего является речь. Частоты речевых сигналов 16 – 20 000 Гц. Один и тот же звук разные люди произносят по-разному (своего рода речевой почерк). Звуки речи не одинаково информативны: гласные содержат мало информации о смысле речи, а глухие согласные наиболее информативны.

Мерой силы звукового ощущения является громкость звука. Минимальная громкость соответствует порогу слышимости, максимальная – порогу болевого ощущения. Оба порога зависят от частоты звука. Человеческому уху свойственно изменение порога слышимости: в условиях тишины слышен писк комара, а в условиях шума трудно услышать громкую речь.

Качество речи оценивается ее разборчивостью, представляющей собой статистическую характеристику речи, принимаемой на фоне шумов. Разборчивость — это отношение числа правильно понятых элементов речи (звуков, слогов, слов) к общему числу переданных по каналу элементов. Она может характеризовать качество канала только в среднем значении, допуская флуктуации в ту или иную сторону. Разборчивость речи определяется экспериментально с помощью так называемых артикуляционных испытаний.

Объективные измерительные и расчетные оценки разборчивости речи могут производиться с помощью вычисления разборчивости формант. Формантами называются максимумы текущего спектра речи, которые заполняют весь речевой диапазон. Доказано, что восприятие человеком формант обладает свойством аддитивности, т. е. каждый участок речевого диапазона вносит свой вклад в общую разборчивость речи. В акустических измерениях используются октавные или третьоктавные частотные полосы. Для октавного анализа вклады частот русской речи равны следующим значениям:

- Частотная полоса, кГц 0,25 0,5 1 2 4 8
- Разборчивость формант, % 6,7 12,5 21,2 29,4 25 5,2

От качественного приема (без искажений и помех) каждой частотной полосы зависит суммарная разборчивость. Предельное значение разборчивости формант, при которой возможно понимание смысла речевого сообщения, равно 15 %, что соответствует 25 %-й разборчивости слогов. Задача оценки канала утечки сводится к измерению или

вычислению разборчивости речи и сравнению полученного значения с предельным. Важным является то, какое качество принятого сигнала может обеспечить используемый канал. Для оценки акустического канала при работе с речевой 67 информацией применяется такая характеристика, как разборчивость речи.

Она зависит от следующих факторов:

• ослабления речи в канале;
• реверберации звука;
• уровня вибрационных и акустических шумов в местах установки датчиков;
• чувствительности самих датчиков.

Оперативная оценка этих факторов осложняется тем, что вибрационные и акустические сигналы не поддаются точному расчету. Качество каналов съема оценивают экспериментальным путем с помощью акустических измерений, имитирующих ситуацию контроля информации.

Шумы и помехи, возникающие в месте установки датчика, вызываются многочисленными источниками: автомобильным транспортом, работой механических машин, технических средств в помещениях, разговорами в смежных помещениях и т. п. Характерная особенность шумов — их нестационарность, т. е. изменение уровня времени. Эти изменения зависят от времени суток (вечером уровни шумов намного меньше, чем днем), от дня недели (в выходные дни уровни шумов снижаются), от погодных условий.

Маскирующие свойства помех проявляются тем сильнее, чем больше их превышение над полезным сигналом во всей полосе частот речевого диапазона. Наибольшие шумы — уличные, которые создаются автомобильным транспортом, листвой (при наличии ветра), а также дворовые. В здании источниками шумов являются люди (разговоры, шаги), работа механизмов, водопровода, лифта. Средние значения акустических шумов на улице составляют 60...75 дБ и зависят от интенсивности движения автомашин в районе расположения объекта. Разница в уровне шумов от максимального до минимального может составлять до 30 дБ. Следует иметь в виду, что существующая норма допустимого уровня акустических шумов в рабочих помещениях равна 50 дБ. Этот уровень можно брать в качестве расчетного, если неизвестны конкретные показатели шумности в смежных посторонних помещениях. Все приведенные значения шумов даны для широкополосных источников помех.

Акустические колебания в помещении складываются из шумов источников, находящихся внутри помещения, и шумов источников вне помещения. Основные пути прохождения акустических волн из помещения:

• воздушный перенос: прохождение через открытые окна, двери, щели, поры, вентиляционные воздуховоды;
• материальный перенос: прохождение через материал стены или по трубам отопления, газопровода, водопровода в виде продольных колебаний;
• мембранный перенос: передача колебаний посредством поперечных колебаний перегородки (стекла, стены и пр.).

При рассмотрении первого пути говорят об акустическом канале утечки, второй и третий образуют вибрационный канал. В воздушных каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные и направленные микрофоны, которые соединяются с диктофонами или специальными минипередатчиками.

Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют закладными устройствами или акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по

радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т. п. В этом случае прием осуществляется, как правило, на специальные приемные устройства. Особого внимания заслуживают закладные устройства, прием информации с которых можно осуществить с телефонного аппарата.

Необходимо отметить, что акустический канал может быть источником утечки не только речевой информации. В литературе описаны случаи, когда с помощью статистической обработки акустической информации с принтера или клавиатуры удавалось перехватывать компьютерную текстовую информацию, в том числе осуществлять съем информации по системе централизованной вентиляции. В вибрационных, или структурных, каналах утечки информации средой распространения акустических сигналов является не воздух, а конструкции зданий (стены, потолки, полы), трубы водо- и теплоснабжения, канализации и другие твердые тела. В этом случае для перехвата акустических сигналов используются контактные, электронные (с усилителем) и радиостетоскопы (при передаче по радиоканалу).

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких как стекла окон, зеркал, картин и т. п., создается оптико-электронный, или лазерный, канал утечки акустической информации. Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие обычно в ближнем инфракрасном диапазоне волн и известные как «лазерные микрофоны».

Дальность перехвата составляет несколько сотен метров. Меры по защите объекта, как правило, направлены на перекрытие возможных каналов съема с помощью инженерных средств, проведение работ по звукоизоляции (для уменьшения воздушного и материального переноса звука через перегородки следует делать их слоистыми, подбирая материалы с резко отличающимися акустическими сопротивлениями, для уменьшения мембранного переноса стены делают массивными и т. д.) и зашумлению строительных конструкций защищаемого здания с помощью специального 69 генератора помех. При проектировании такой системы крайне важна точная оценка объекта, так как виброакустическими методами съема информации пользуются квалифицированные профессионалы с применением самой высококачественной техники.

Преобразователи аудиоинформации Преобразователем является прибор, который преобразует изменения одной физической величины в изменения другой. Акустическая энергия, возникающая при разговоре, может вызвать акустические (т. е. механические) колебания элементов электронной аппаратуры, что в свою очередь приводит к появлению или изменению электромагнитного излучения. Любой преобразователь характеризуется определенными параметрами.

Наиболее важными из них являются:

• чувствительность – отношение изменения выходного сигнала к изменению сигнала на его входе;

• разрешающая способность – наибольшая точность, с которой осуществляется преобразование;

• линейность – равномерность изменения выходного сигнала в зависимости от входного;

• инертность (время отклика) – время установления выходного сигнала в ответ на изменение входного сигнала;

• рабочая полоса частот – частотный диапазон, в пределах которого воздействие на входе преобразователя создает на выходе допустимый уровень сигнала.

По физической природе имеется значительное количество различных первичных преобразователей, среди которых выделяются следующие группы:

• индуктивные;

• емкостные;

• пьезоэлектрические;

• оптические преобразователи.

Наиболее чувствительными к акустическим воздействиям элементами радиоэлектронной аппаратуры являются катушки индуктивности и конденсаторы переменной емкости.

1. Индуктивные преобразователи. Микрофонный эффект. Рассмотрим акустическое воздействие на катушку индуктивности с сердечником. Механизм и условия возникновения ЭДС индукции в такой катушке сводятся к следующему. Под воздействием акустического давления появляется вибрация корпуса и обмотки катушки. Вибрация вызывает колебания проводов обмотки в магнитном поле, что и приводит к появлению 70 ЭДС индукции на концах катушки. Она зависит от вектора магнитной индукции, магнитной проницаемости сердечника, угла между вектором и осью катушки, угла между вектором и осью сердечника и площадей поперечных сечений сердечника и катушки. Данный эффект непосредственно используется в электродинамических микрофонах, поэтому получил название микрофонного эффекта.

Индуктивные преобразователи подразделяются на электромагнитные, электродинамические и магнитострикционные. К электромагнитным преобразователям относятся такие устройства как громкоговорители, электрические звонки (в том числе и вызывные звонки телефонных аппаратов), электрорадиоизмерительные приборы. Типичный образец индуктивного акустоэлектрического преобразователя – электромеханический вызывной звонок телефонного аппарата, микрофонный эффект которого проявляется при положенной телефонной трубке. По тому же принципу образуется микрофонный эффект и в отдельных типах электромеханических реле различного назначения. Акустические колебания воздействуют на якорь реле.

Колебания якоря изменяют магнитный поток реле, замыкающийся по воздуху, что приводит к появлению на выходе катушки реле ЭДС микрофонного эффекта. Динамические головки прямого излучения, устанавливаемые в абонентских громкоговорителях, имеют достаточно высокую чувствительность к акустическому воздействию и довольно равномерную в речевом диапазоне частот амплитудно-частотную характеристику, что обеспечивает высокую разборчивость речевых сигналов. В магнитоэлектрическом измерительном приборе имеются подвижный постоянный магнит и подвижная рамка, которая поворачивается вокруг своей оси под воздействием собственного магнитного поля, создаваемого измеряемым напряжением, и магнитного поля постоянного магнита. Рамка соединена со стрелкой, конец которой перемещается по шкале измерения. Если акустические колебания воздействуют на рамку, она вращается под их давлением и на ее концах возникает ЭДС индукции.

Практически аналогичная ситуация будет при воздействии акустических колебаний на электромагнитный измерительный прибор. Различие между магнитоэлектрическим и электромагнитным приборами сводится к тому, что в электромагнитном приборе вместо постоянного магнита используется электромагнит. Следует отметить, что ЭДС микрофонного эффекта возникает и может использоваться в состоянии покоя прибора, когда он не применяется для конкретных измерений. Примерами индукционных

акустоэлектрических преобразователей являются различные трансформаторы (повышающие, понижающие, входные, выходные, питания и др.).

Трансформатор состоит из двух (или более) изолированных друг от друга катушек (обмоток) с разными числами витков и замкнутого сердечника из мягкой стали или феррита. Акустическое влияние на сердечник и обмотку трансформатора (например, на входной трансформатор усилителя звуковых частот) приведет к появлению микрофонного эффекта. Если ЭДС индукции появляется в первичной обмотке, то во вторичной обмотке она увеличивается в коэффициент трансформации раз.

Магнитострикция — изменение размеров и формы кристаллического тела при намагничивании — вызывается изменением энергетического состояния кристаллической решетки в магнитном поле и, как следствие, расстояний между узлами решетки. Наибольших значений магнитострикция достигает в ферро- и ферритомагнетиках, в которых магнитное взаимодействие частиц особенно велико. Обратное по отношению к магнитострикции явление — Виллари-эффект, т. е. изменение намагничиваемости тела при его деформации. Виллари-эффект обусловлен изменением под действием механических напряжений доменной структуры ферромагнетика, определяющей его намагниченность. В усилителях с очень большим коэффициентом усиления входной трансформатор на ферритах способен преобразовывать механические колебания в электрические.

2. Емкостные преобразователи.

Емкостные преобразовывающие элементы превращают изменение емкости в изменение электрического потенциала, тока, напряжения. Емкость конденсатора зависит от расстояния между пластинами. Воздействующее на пластины акустическое давление, изменяя расстояние между пластинами, приводит к изменению емкости. Конденсаторы переменной емкости с воздушным диэлектриком являются одним из основных элементов перестраиваемых колебательных контуров генераторных систем. Они устроены так, что система пластин вдвигается в другую систему пластин, образуя конденсатор переменной емкости. Изменяющееся акустическое давление, воздействуя на такой конденсатор, изменяет его емкость, а следовательно, и характеристики устройства, в котором он установлен.

3. Пьезоэлектрический преобразователь. Изучение свойств твердых диэлектриков показало, что некоторые из них поляризуются не только с помощью электрического поля, но и в процессе деформации при механических воздействиях на них. Поляризация диэлектрика при механическом воздействии называется прямым пьезоэлектрическим эффектом. Этот эффект имеется у кристаллов кварца и у всех сегнетоэлектриков. У пьезокристаллов наблюдается и обратное явление. Если пластину, вырезанную из пьезокристалла, поместить в электрическое поле, зарядив металлические обкладки, то она поляризуется и деформируется, например сжимается. При перемене направления внешнего электрического поля сжатие пластинки сменяется ее растяжением (расширением). Такое явление называется обратным пьезоэлектрическим эффектом. Кварцевые пластины широко используются в пьезоэлектрических микрофонах, охранных датчиках, стабилизаторах, генераторах электрического микрофона.

4. Оптические преобразователи. К оптическим преобразователям относятся приборы, преобразующие световую энергию в электрическую и обратно. Что касается технических каналов утечки информации, то в оптических системах опасным является акустооптический эффект. Акустооптический эффект — это явление преломления, отражения или рассеяния света, вызванное упругими деформациями стеклянных отражающих поверхностей или волоконно-оптических кабелей под воздействием

звуковых колебаний. Волоконные световоды как преобразователи механического давления в изменение интенсивности света являются источником утечки акустической информации за счет акустооптического (или акустоэлектрического) преобразования — микрофонного эффекта в волоконно-оптических системах передачи информации (используется также в охранных системах). Основным элементом оптического кабеля волоконно-оптических систем является волоконный световод в виде тонкого стеклянного волокна цилиндрической формы. Волоконный световод имеет двухслойную конструкцию и состоит из сердцевины и оболочки с различными оптическими характеристиками (показателями преломления). Сердцевина служит для передачи электромагнитной энергии. Назначение оболочки — создание лучших условий отражения на границе сердцевина–оболочка и защита от излучения в окружающее пространство. Передача волны по световоду осуществляется за счет отражений ее от границы сердечника и оболочки, имеющих разные показатели преломления. В современных волоконно-оптических системах в процессе передачи информации используется модуляция источника света по амплитуде, интенсивности и поляризации. Внешнее акустическое воздействие на волоконно-оптический кабель приводит к изменению его геометрических размеров (толщины), что вызывает изменение пути движения света, т. е. приводит к изменению интенсивности, причем пропорционально значению этого давления. При слабом закреплении волокон в разъемном соединителе световодов проявляется акустический эффект модуляции света акустическими полями. Акустические волны вызывают смещение соединяемых концов световода относительно друг друга. Таким образом осуществляется амплитудная модуляция излучения, проходящего по волокну.

В контролируемой зоне следует свести к минимуму количество имеющихся преобразователей. Меры защиты от утечки информации через аудиопреобразователи те же, что и меры защиты от утечки через электромагнитные каналы.

Практическая часть 1:

Подготовиться к семинарскому занятию. Выбрать одну из предложенных тем:

- Электромагнитные каналы утечки
- Визуально-оптические каналы утечки
- Информационные каналы утечки информации
- Технические каналы утечки информации

Практическая часть 2:

Методические указания для студентов по выполнению практического задания

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифровкой, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-расшифровки. В соответствии со стандартом ГОСТ 28147-89 под **шифром** понимают совокупность обратимых

преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифровки осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровке сообщений. В **асимметричных** криптосистемах для шифрования данных используется один (общедоступный) ключ, а для расшифровки – другой (секретный) ключ.

Симметричные криптосистемы

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам:

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово «ЛУНАТИК», получим следующую таблицу:

Л	У	Н	А	Т	И	К			А	И	К	Л	Н	Т	У
4	7	5	1	6	2	3			1	2	3	4	5	6	7
Н	О	Н	С	Б	Н	Я			С	Н	Я	Н	Н	Б	О
Е	Е	О	Я	О	Е	Т			Я	Е	Т	Е	О	О	Е
Я	С	В	Е	Л	П	Н			Е	П	Н	Я	В	Л	С
С	Т	И	Щ	Е	О	Ы			Щ	О	Ы	С	И	Е	Т
Н	А	Т	Е	Е	Н	М			Е	Н	М	Н	Т	Е	А

До перестановки После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке перестановки проводятся в обратном порядке. Например, сообщение “Приезжаю_шестого” можно зашифровать следующим образом:

	2	4	1	3			1	2	3	4			1	2	3	4
4	П	Р	И	Е		4	И	П	Е	Р		1	А	З	Ю	Ж
1	З	Ж	А	Ю		1	А	З	Ю	Ж		2	Е	_	С	Ш
2	_	Ш	Е	С		2	Е.	_	С	Ш		3	Г	Т	О	О
3	Т	О	Г	О		3	Г	Т	О	О		4	И	П	Е	Р

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			_	Ж	А	С
4	15	14	1			Е	Г	О	П

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5- 250000.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение: СОВЕРШЕННО СЕКРЕТНО

Ключ: 3143143143143143143

Шифровка: ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит):

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

Гаммирование

Процесс шифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i$=$Г(ш)_i$+$Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифровки сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i$=$Г(ш)_i$+$Т(ш)_i$.

Асимметричные криптосистемы

Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем P G.
2. Получатель выбирает секретный ключ - случайное целое число X P.
3. Вычисляется открытый ключ $Y= G^x \bmod P$.
4. Получатель выбирает целое число K, 1P-1.
5. Шифрование сообщения (M): $a= G^K \bmod P$, $b=Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Алгоритм создания открытого и секретного ключей:

1. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $n=p*q$ и функцию Эйлера $\varphi(n)=(p-1)(q-1)$.
2. Получатель выбирает целое число e (1e $\varphi(n)$), взаимно простое со значением функции $\varphi(n)$.

Пара чисел **(e,n)** публикуется в качестве **открытого ключа**.

1. Получатель вычисляет целое число d, которое отвечает условию: $e*d=1(\text{mod } \varphi(n))$.

Пара чисел **(d,n)** является **секретным ключом**.

Шифрование сообщения с использованием открытого ключа:

Если m – сообщение (сообщениями являются целые числа в интервале от 0 до n-1), то зашифровать это сообщение можно как $\mathbf{c=m^e \bmod(n)}$.

Дешифрование сообщения с использованием секретного ключа:

Получатель расшифровывает, полученное сообщение c: $\mathbf{m=c^d \bmod (n)}$.

Задание

Практическая работа состоит из двух частей:

Часть 1 – применение одного из алгоритмов симметричного шифрования;

Часть 2 – шифрование с использованием алгоритма RSA.

Порядок выполнения работы:

Часть 1:

1. Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество.
2. Выполнить проверку, расшифровав полученное сообщение.

Часть 2:

1. Написать программу, реализующую алгоритм шифрования и дешифрования сообщения RSA. Входные данные: открытый и секретный ключи (значения n, e, d) и сообщение (m).
2. Используя заданные значения p, q, e, d (см. вариант) зашифровать и дешифровать сообщения m_1, m_2, m_3 (см. вариант).

Практическое занятие № 14-17

Тема: Настройка работоспособности системы и отчет по оценке работоспособности системы

Цель: оценить и настроить работоспособность системы, подготовить подробный отчет по работоспособности системы и записать в тетрадь

Практическая часть 1:

Оценка работоспособности технической системы.

При оценке работы технической системы используют как структурные, так и диагностические параметры. Так же учитывают скоростные и динамические характеристики как системы в целом, так и ее подсистем. Определяя значения параметров и характеристик, оценивают состояние системы и определяют возможность ее дальнейшей эксплуатации, при этом, из всей совокупности параметров выделяют следующие:

$Y_{iн}$, $S_{iн}$ ($i = 1,\ldots, n$) - номинальные значения рабочих (структурных) и диагностических параметров, которые определяются конструкторской документацией и качеством изготовления изделия

Y_{in}, S_{in} ($i = 1,\ldots, n$) - предельные значения рабочих (структурных) и диагностических параметров, превышения которых приводит к отказу системы или определяет порог использования системы.

$Y_{inд}$, $S_{inд}$ ($i = 1,\ldots, n$) - предельно-допустимые значения рабочих (структурных) и диагностических параметров, которые являются близкими к предельным и фиксируются заранее. Например, если глубина протектора шин легкового автомобиля менее 1,5 мм, то их дальнейшая эксплуатация должна быть прекращена.

Y_i , S_i (i = 1,…, n) - текущие значения рабочих и структурных параметров, определяемых в период эксплуатации, по которым производится оценка состояния системы, прогнозируется остаточный ресурс.

Перечень неисправностей и условий, при которых запрещена эксплуатация транспортных средств, устанавливается на федеральном уровне нормативными актами.

Техническое состояние автомобиля определяется текущим значением рабочих параметров Y_i, которые определяются прямым или косвенным методом (Рис 1.4)

		Методы О.Т.С.		
Прямой – непосредственное изменение конструктивных параметров		Косвенный (диагностический) – по измерениям диагностических параметров		

износ тормозных накладок, Y_i	←	S_i -длина тормозного пути	
дисков, барабанов Y_{ind}	←	S_{ind} -ход педали тормоза	
износ поршневой группы Y_{in}	←	S_{in} –компрессия, расход масла	

Рис 1.4 Прямые и косвенные методы определения рабочих параметров Свойства диагностических параметров

При определении технического состояния автомобиля, как мы отмечали выше, оценку работоспособности его можно производить непосредственно по значениям рабочих параметров, а так же по значениям диагностических параметров. Для определения значений рабочих параметров часто приходится производить разборку того или иного агрегата, что связано с высокой трудоемкостью данных работ. Желательно, чтобы диагностические параметры имели следующие свойства:

- ***однозначность*** определяется тем, что при изменении параметра Y_i в пределах $Y_{iн}$ … Y_{in} имеется соответствие $Y_i \leftrightarrow S_i$ т.е. одному значению Y_i соответствует только одно значение S_i ,где S_i –диагностический параметр;

- ***чувствительность*** характеризуется тем, что приращение ΔS_i по отношению к изменению конструктивного параметра является постоянным, т.е. $\Delta Y_i/\Delta S_i$ =const либо изменяется очень незначительно;

- ***стабильность***устанавливает возможную величину отклонения диагностического параметра от своего расчетного;

- ***доступность и удобство измерения*** предусматривает измерение параметров без разборки подсистем узлов агрегата, либо незначительную разборку узла;

- ***информативность*** позволяет обеспечить через измерение диагностических параметров S_i достаточно полную информацию о параметрах системы Y_i.

Заметим, что чем больше число измеряемых диагностических параметров, тем более полной является информация о состоянии технической системы, но при этом повышается трудоемкость и стоимость диагностирования. При выборе диагностических параметров необходимо предусмотреть, чтобы они были независимы. Как правило, выбор этих параметров осуществляется на основе накопленного опыта с использованием рекомендации, содержащихся в нормативно-технической документации. Многочисленные диагностические параметры условно можно разделить на 2 класса:

1. Диагностические параметры выходных характеристик рабочих процессов, которые характеризуют основные функциональные свойства автомобиля и его систем. К ним можно отнести мощность двигателя, максимально допустимую скорость, расход топлива, рабочую температуру двигателя, тормозной путь.

2. Диагностические параметры сопутствующих процессов, которые сопровождают работу автомобиля в целом и его подсистем к ним можно отнести: уровень шума и вибрации, содержание продуктов износа деталей в масле и т.д.

Средства диагностирования обычно разделяют на внешние и встроенные (Таблица 1.4).

Таблица 1.4 Классификация средств диагностирования

Средства диагностирования	
Внешние	Встроенные
стационарные	информационные
передвижные	стационарные
переносные	программируемые

К внешним следует отнести различные стенды, такие как: стенд проверки установки углов схождения и развала, тормозной стенд, диагностический стенд. Примером переносного средства диагностирования является прибор для определения уровня загрязнения в отработанных газах.

Встроенные средства диагностирования являются конструкционными элементами автомобиля. Они позволяют контролировать некоторые рабочие параметры автомобиля, сигнализируют о возможности наступления отказа, либо непосредственно о самом отказе.

Следует заметить, что прямой и косвенный методы диагностирования автомобиля в большинстве случаев используются совместно с целью получения минимальных затрат на определение технического состояния автомобиля. Например, процесс диагностирования двигателя начинают с использования косвенного метода по значению параметра типа S_i, и, если результат выполненного диагностирования является неудовлетворительным, то используют прямой метод с частичной разборкой двигателя.

Контрольные вопросы.

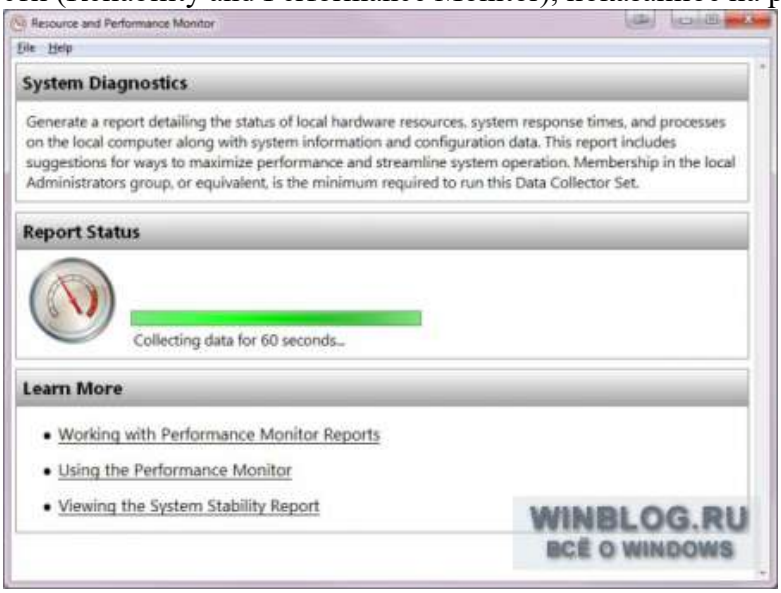
1. Приведите примеры технических систем находящихся на кухне вашей квартиры?
2. Какие этапы жизненного цикла автомобиля имеют отношение к вашей специальности (специальность 190603)?
3. Что такое база знаний? Что она включает?
4. Что такое целеполагание (как этап жизненного цикла)?
5. Какие факторы влияют на эксплуатацию автомобиля ?
6. Почему (в отличие от плановой) в условиях рыночной экономики улучшились качество и быстрота сервиса ?
7. Какие виды работ включает техническое обслуживание и сервис?
8. Какая разница между сервисом и техническим обслуживанием?
9. Назовите основные показатели качества?
10. Что такое наработка двигателя?
11. Какая разница между предельным состоянием и предельно допустимым состоянием?
12. Какая разница между усталостным изнашиванием и усталостным разрушением?
13. Перечислите виды изнашивания?
14. В чем общность и отличие понятий «исправность» и «работоспособность» объекта?
15. Что такое диагностические параметры? Приведите примеры этих параметров.
16. Перечислите требования к диагностическим параметрам?
17. Что такое однозначность диагностических параметров?
18. Что такое чувствительность диагностических параметров?

Практическая часть 2:

Создание отчета о работоспособности системы

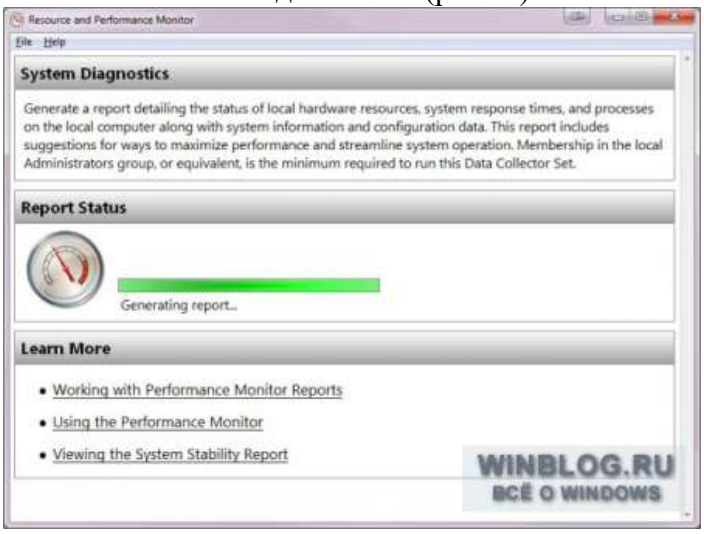
Запустить создание отчета о работоспособности системы можно из раздела «Дополнительные инструменты» (Advanced Tools) утилиты «Счетчики и средства

производительности» (Performance Information and Tools) в Панели управления (Control Panel). Но куда проще ввести в строке поиска меню «Пуск» (Start) команду perfmon /report и нажать [Enter]. При этом потребуется подтвердить выполнение операции в окне контроля учетных записей, после чего появится окно Монитора ресурсов и производительности (Reliability and Performance Monitor), показанное на рис. A.

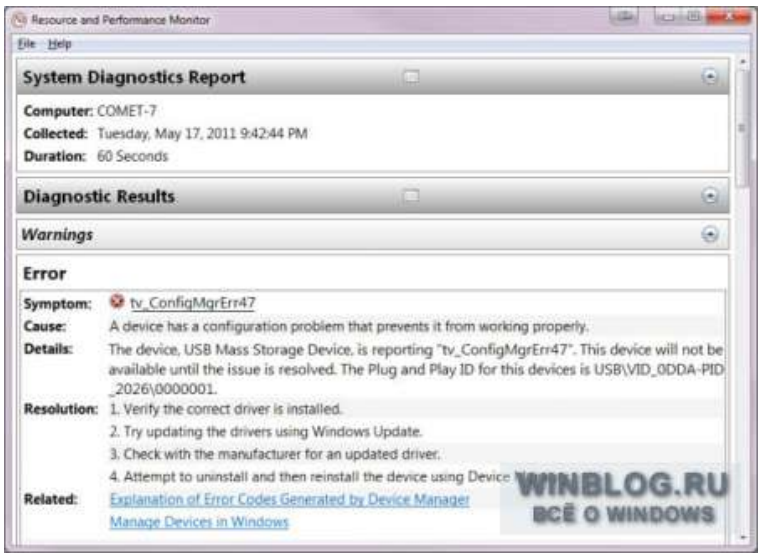


Как видите, в разделе «Состояние отчета» (Report Status) сообщается, что средство диагностики системы будет собирать данные в течение 60 секунд. В этот момент можно запустить выполнение задачи, с которой связана та или иная неполадка. Если проблему удастся воспроизвести, информация о ней будет содержаться в отчете.

Для проверки я подключил к системе USB-кардридер 8-в-1, с которым у меня были неполадки. Через 60 секунд в разделе «Состояние отчета» появилось сообщение о том, что средство диагностики системы создает отчет (рис. B).



Готовый отчет отображается в окне Монитора ресурсов и производительности (рис. C). В отчете содержатся сведения обо всех ошибках, обнаруженных в процессе сбора данных.



Как видите, в отчет попала информация и о моем проблемном кардридере. Она представлена в разделе «Ошибка» (Error). Кроме того, утилита обнаружила несколько других проблем, о которых я и не подозревал.

Сведения о каждой обнаруженной неполадке в разделе «Предупреждения» (Warnings) разбиты на пять пунктов:

• **«Симптом» (Symptom):** системное сообщение об ошибке. Симптом представлен в виде ссылки, по которой можно посмотреть более подробные сведения.

• **«Причина» (Cause):** описание условий, при которых возникает ошибка.

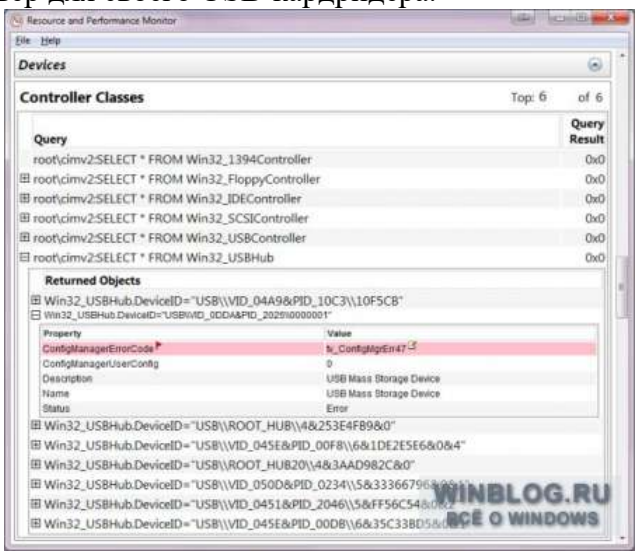
• **«Сведения» (Details):** более подробная информация об ошибке.

• **«Разрешение» (Resolution):** набор базовых рекомендаций по разрешению обнаруженной проблемы.

• **«Связанный» (Related):** ссылки на статьи с сайта Microsoft, касающиеся данной проблемы.

В моем случае по ссылкам открылась страница справки по Windows Vista и несуществующая страница на сайте Microsoft TechNet. Судя по всему, с этими ссылками разработчики промахнулись.

Зато по ссылке в пункте «Симптом» открылся раздел «Устройства | Классы контроллеров» (Devices | Controller Classes, рис. D), где я обнаружил несколько полезных формулировок для поиска в Google. В конечном итоге выяснилось, что мне надо было просто обновить драйвер для своего USB-кардридера.



Практическая часть 3:

Пошаговая инструкция полного тестирования вашего компьютера

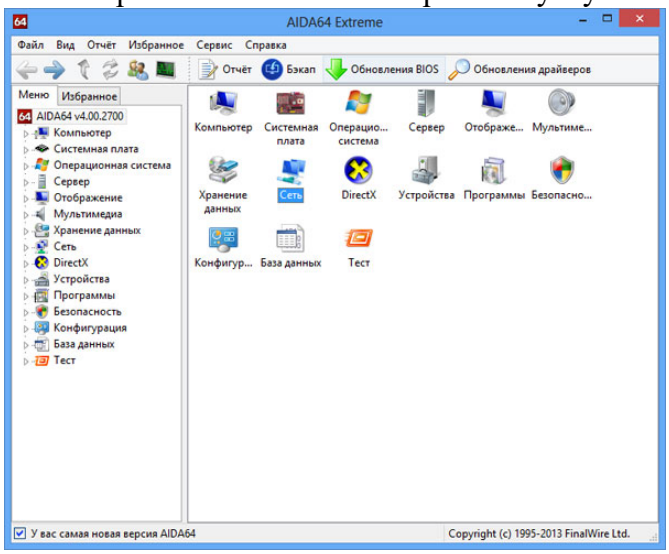
Тестирование компьютера необходимо для быстрого выявления любых неполадок в работе системы как на программном, так и на аппаратном уровне.

Если программа-тестировщик показывает результат, который отличается от нормального, это свидетельствует о том, что одно или несколько устройств работают неверно.

Чтобы получить более точный результат диагностики, следует проверять компьютер несколькими разными программами.

Диагностика с помощью утилиты Aida64

Данная программа способна предоставить отчет о результатах работы сразу всех компонентов системы (железа и программ). Утилита является самой популярной программой для тестирования персональных компьютеров и ноутбуков.



Внешний вид интерфейса программы AIDA64

Интерфейс приложения очень простой, поэтому каждый пользователь сможет провести тесты необходимого компонента или всей системы в целом.

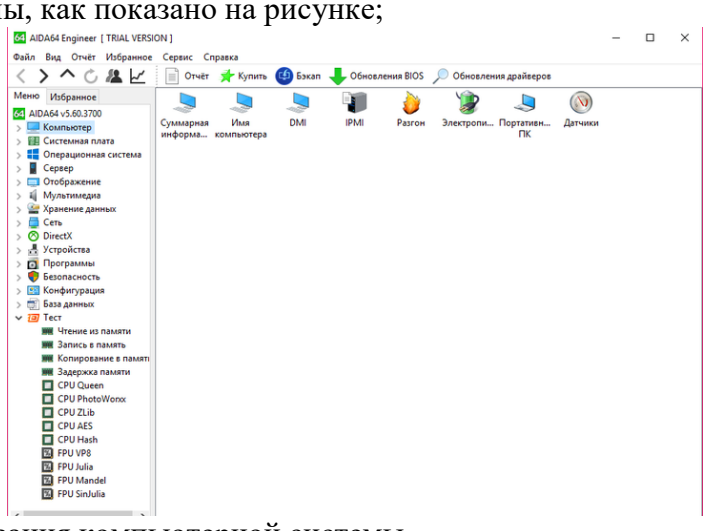
Скачать программу можно по ссылке с официального сайта разработчиков: http://www.aida64.ru/download.

Интерфейс приложения представлен на русском языке.

Проведем общее сканирование компьютера на производительность и возможные неполадки с помощью данного приложения.

Чтобы начать процесс тестирования, следуйте инструкции:

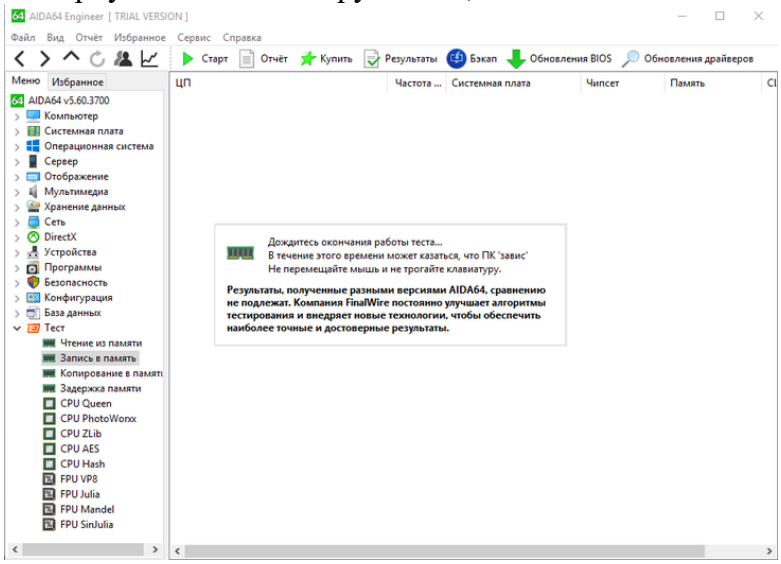
Откройте программу и нажмите на вкладку «Тест», которая находится в левом нижнем углу программы, как показано на рисунке;



Начало тестирования компьютерной системы

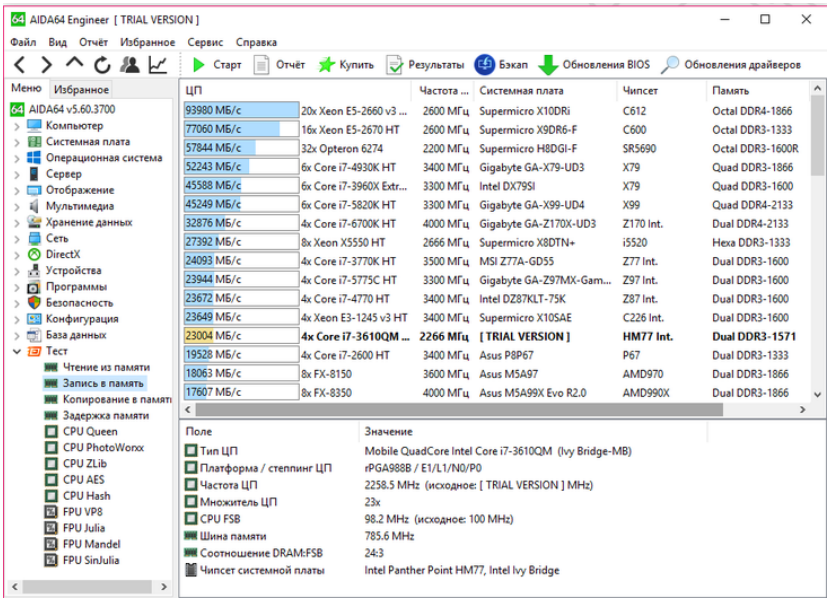
На вкладке тестирования представлены все возможные варианты сканирования таких компонентов, как память. Также можно провести диагностику процесса записи в память и задержки в памяти.

Чтобы протестировать один из элементов, выберите его на него, а затем нажмите на кнопку «Старт» вверху на панели инструментов;



Начало процесса тестирования записи в память

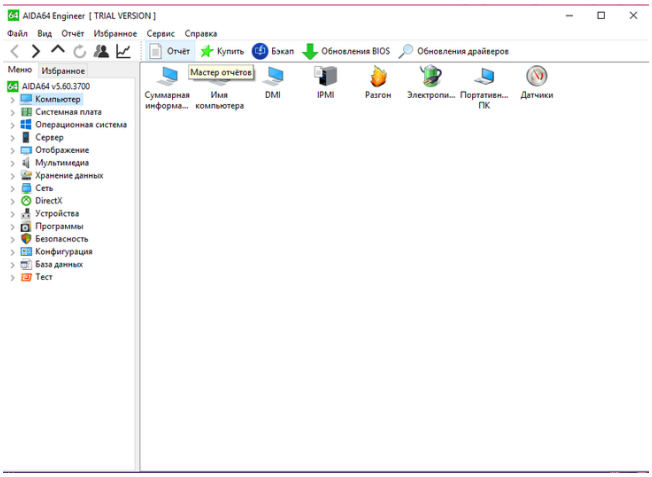
Далее программа покажет мощность процессора в сравнении с другими популярными моделями и основные характеристики системы, а также возможные неполадки;



Результаты тестирования работы процессора и записи в память

Следуйте нижеприведенной инструкции, чтобы получить подробный отчет о системе:

Зайдите в основное окно программы и нажмите на клавишу «Отчет», которая расположена на главной панели инструментов;

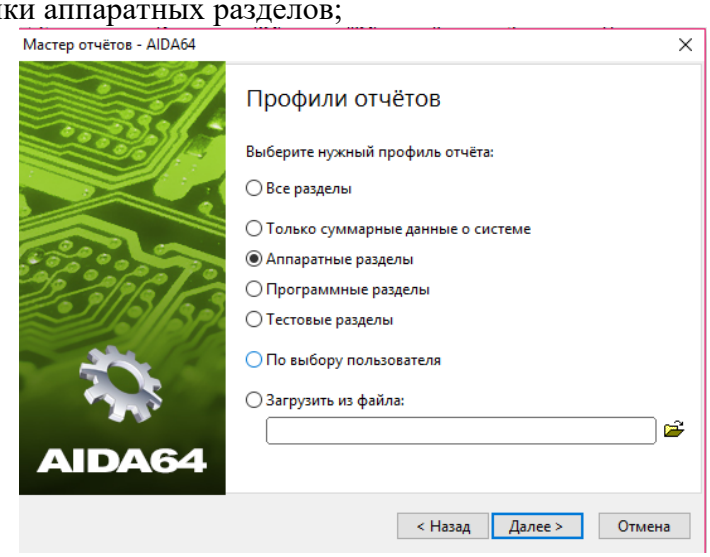


Начало формирования отчета о производительности компьютерной системы

Откроется мастер отчетов. Нажмите на клавишу далее для более детальной настройки исходящего отчета;

Открытие мастера отчетов

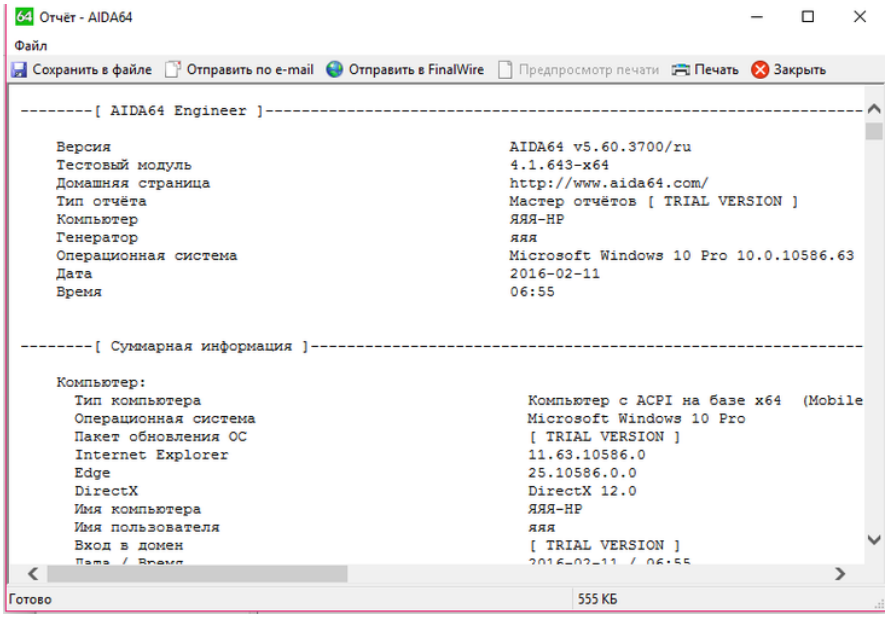
Выберите направление отчета. Он может быть составлен на основе программных или аппаратных компонентов. В данном случае аппаратный отчет будет состоять из результатов диагностики аппаратных разделов;



Выбор профиля отчета

Затем выберите удобный для вас формат отчета и дождитесь завершения формирования конечного документа;

Пример текстового формата исходного отчета об аппаратных разделах представлен на рисунке ниже.



Конечный результат тестирования в виде текстового отчета

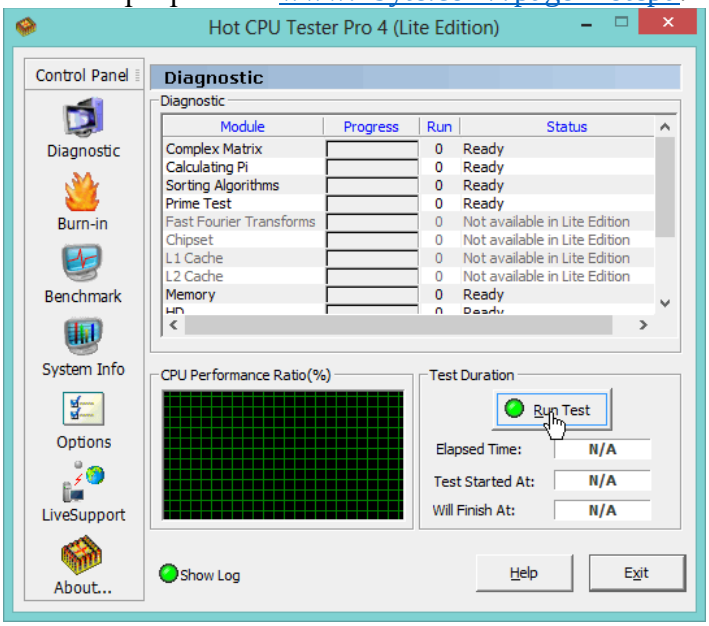
Тестирование процессора. Программа CPU Tester

Тестирование процессора способно показать его детальные параметры. Также с помощью такого теста можно определить существующие неполадки центрального процессора, которые тормозят работу компьютера.

Совет! Если вы недавно приобрели компьютер, желательно протестировать процессор и другие аппаратные компоненты, чтобы убедится в правильности всех предоставленных производителем аппаратных характеристик.

Осуществить тестирование процессора можно с помощью программы CPU Tester.

Ссылка для скачивания программы: www.7byte.com/?page=hotcpu.

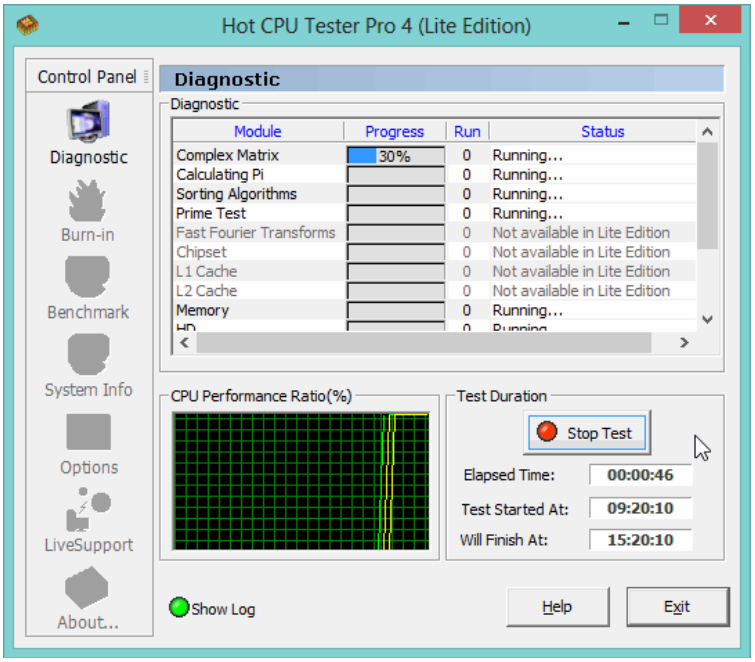


Внешний вид программы CPU Tester

Данная утилита обладает мощным функционалом для тестирования процессора устройства и определения его основных параметров. Также программа способна определить неполадки и неисправности и указать их характер. Утилита также доступна в режиме онлайн.

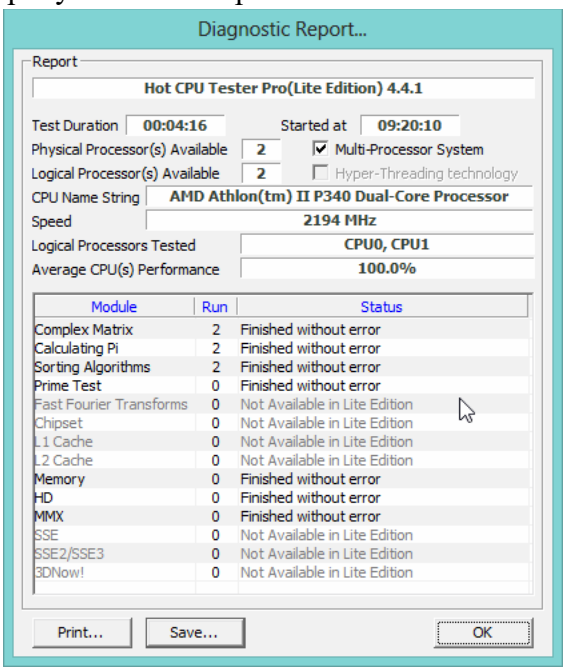
Во время проведения тестирования необходимо закрыть все работающие программы и игры, ведь они будут дополнительно нагружать процессор и конечный результат тестирования не будет соответствовать действительности.

После закрытия всех запущенных программ, нажмите на кнопку «Запустить Тест», чтобы начать процесс проведения и формирования тестирования центрального процессора.



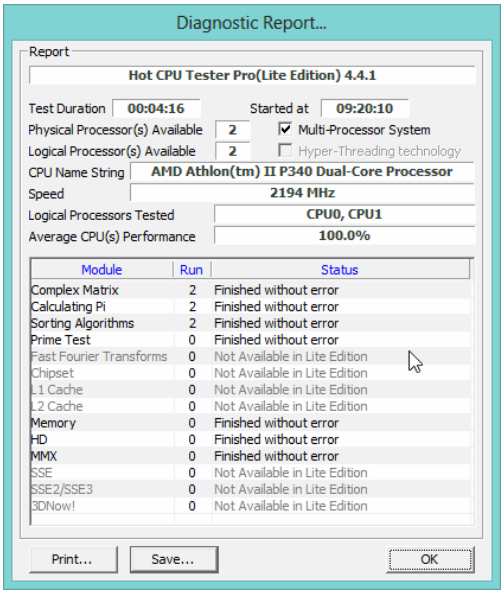
Процесс проведения отчетности

После окончания процесса тестирования программа откроет новое пользовательское окно, в котором будут указан все результаты диагностики и параметры процессора, как показано на рисунке ниже. При желании отчет можно напечатать.



Процесс проведения отчетности

После окончания процесса тестирования программа откроет новое пользовательское окно, в котором будут указан все результаты диагностики и параметры процессора, как показано на рисунке ниже. При желании отчет можно напечатать.



Конечный результат тестирования процессора с помощью программы CPU Tester

В данном примере теста, показано, что процессор работает стабильно, без каких-либо сбоев.

Практическая часть 4:

Тестирование блока питания

Если ваш персональный компьютер слишком быстро нагревается, при этом все вентиляторы прочищены и работают стабильно, необходимо проверить исправность блока питания. Необходимо проверить подачу напряжения к блоку питания.

Откройте крышку компьютера и отключите блок питания от корпуса;

Блок питания компьютера

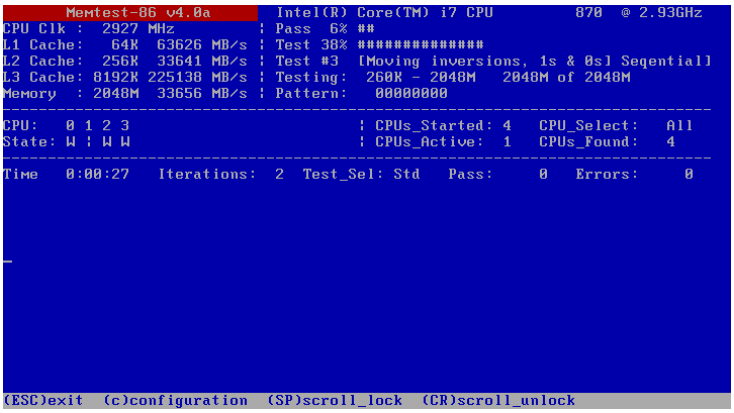
Совет! Чтобы потом закрепить блок питания на прежнее место, можете сфотографировать его первоначальное положение.

Подключите блок питания к вашей сети и протестируйте переключатель.

Чтобы проверить работу блока питания на программном уровне, можно использовать программу speedfan, которая способна регулировать работу блока и управлять режимами работы вентиляторов компьютера.

Тестирование оперативной памяти. Программа Memtest

Для тестирования оперативной памяти лучше всего использовать утилиту Memtest, которая предназначена регулировать работу и определять неисправности в памяти компьютера.



Интерфейс утилиты Memtest

Тестирование проводится следующим образом:

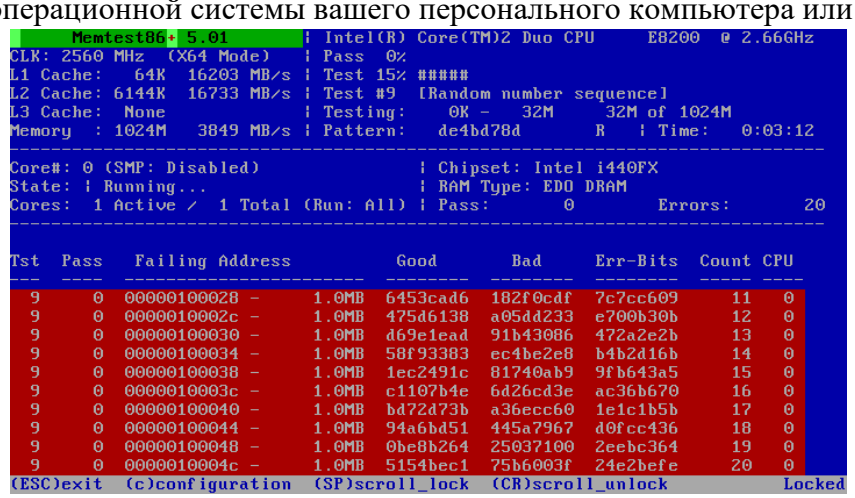
Скачивается и устанавливается программное обеспечение для тестирования на сайте разработчика www.memtest.org;

Затем необходимо создать загрузочный диск или флеш-носитель. Тестирование диска будет проводиться в оперативной памяти, поэтому можно будет определить ее работоспособность;

Необходимо загрузить компьютер с только что созданного диска. Настроить порядок загрузки устройств можно в БИОСе компьютера.

Если процесс тестирования длиться очень долго и не останавливается, это говорит о том, что система работает нормально и оперативной памяти компьютера отсутствуют неисправности.

Если будут найдены какие-либо неполадки, процесс тестирования будет остановлен и пользователь будет уведомлен о найденных ошибках. Затем начнётся процесс запуска операционной системы вашего персонального компьютера или ноутбука.



Пример тестирования оперативной памяти с помощью программы Memtest

Тестирование монитора. Программа IsMyLcdOK

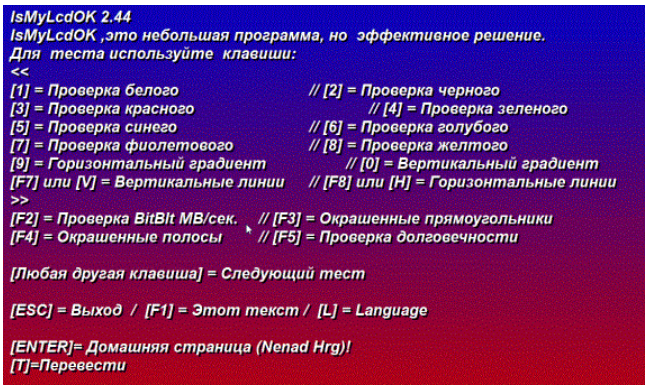
Тестирования монитора проводят, чтобы найти нерабочие или как их еще называют «битые» пиксели. Такие пиксели неспособны передавать цвет или информацию, потому на экранах с маленьким разрешением они будут видны.

Большое количество таких пикселей говорит о том, что монитор некачественный или бракованный.

Лучшая утилита для проверки изображения монитора – это IsMyLcdOK. Данное приложение позволяет пользователю быстро определить количество битых пикселей дисплея.

Процесс тестирования выглядит следующим образом: экран полностью окрашивается в определенный цвет, пользователю необходимо нажать мышкой на любой место для того, чтобы кран окрасился в новый цвет.

Такое изменение цветов помогает невооруженным глазом определить нерабочие пиксели.

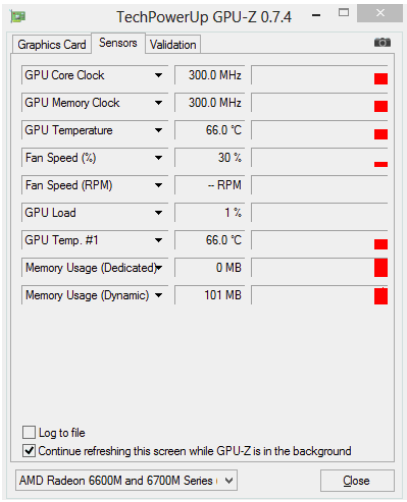


Тестирование видеокарты. Программа FurMark

Видеокарту необходимо регулярно тестировать на наличие неисправностей, особенно если вы владелец игрового компьютера или ноутбука.Протестировать видеокарту поможет бесплатная утилита под названием FurMark.

Скачать можно по ссылке: www.ozone3d.net/benchmarks/fur.

Чтобы начать тестирование видеокарты, нажмите на клавишу «GPU-Z», как показано на рисунке выше.



Практическое занятие № 18-22

Тема: Разработка и применение политики агентского мониторинга для работы с носителями и устройствами.

Цель: разработать и применить агентский мониторинг для работы с носителями и устройствами.

Практическая часть:

Задание 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “Champ” в корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

Внутри созданного подразделения “Champ” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

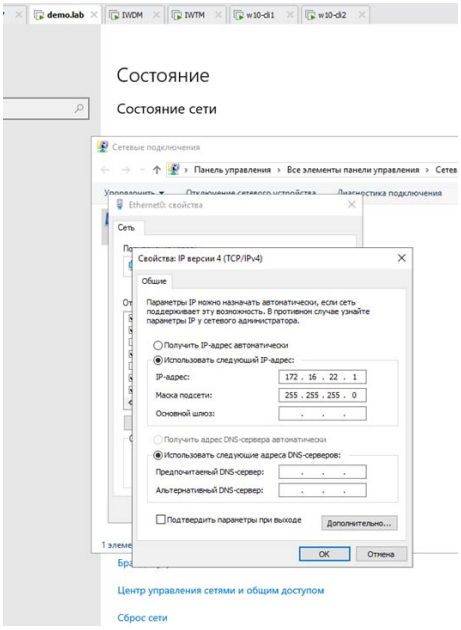
Логин: user-agent1, пароль: xxXX1234, права пользователя домена

Логин: user-agent2, пароль: xxXX1234, права пользователя домена

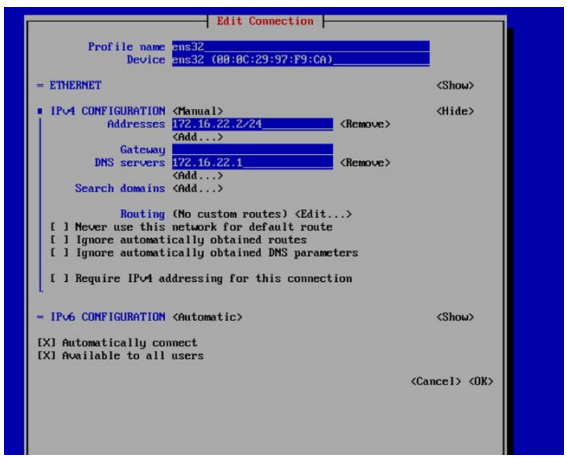
Логин: iw-admin, пароль: xxXX1234, права администратора домена

Логин: iwtm-officer, пароль: xxXX1234, права пользователя домена

Логин: ldap-sync, пароль: xxXX1234, права пользователя домена

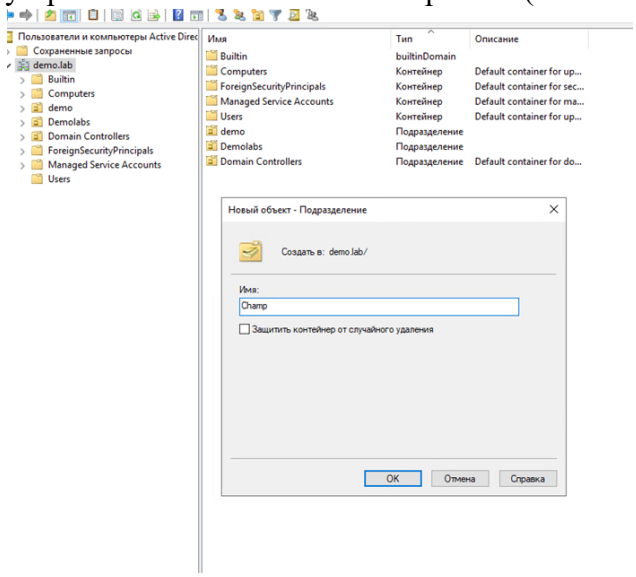


Прописываем – nmtui. Там также проверяем сетевую настройку (действуем по тому же принципу, главное наличие DNS (для дальнейшей работы с краулером). После этого можно пропинговать для проверки (или зайти в браузер>инфовоч., чтобы убедится в том что все работает)

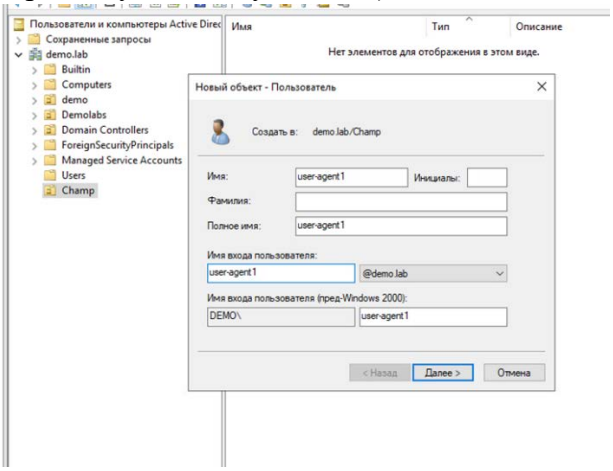


```
[root@iwtm ~]# ping 172.16.22.1
PING 172.16.22.1 (172.16.22.1) 56(84) bytes of data.
64 bytes from 172.16.22.1: icmp_seq=1 ttl=128 time=1.93 ms
64 bytes from 172.16.22.1: icmp_seq=2 ttl=128 time=0.454 ms
64 bytes from 172.16.22.1: icmp_seq=3 ttl=128 time=1.11 ms
^C
--- 172.16.22.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.454/1.165/1.931/0.604 ms
[root@iwtm ~]#
```

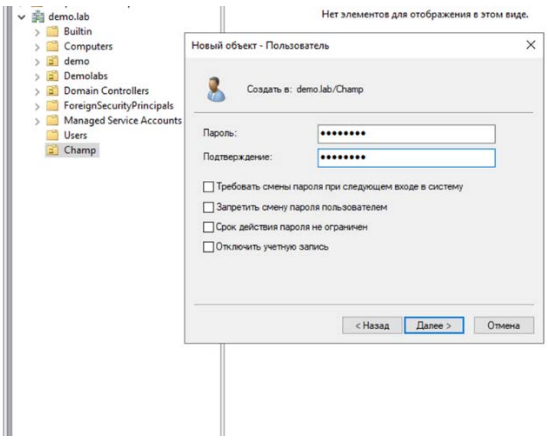
Или же зайти в браузер на demo.lab и там ввести ip iwtm (то есть зайти на инфовоч)



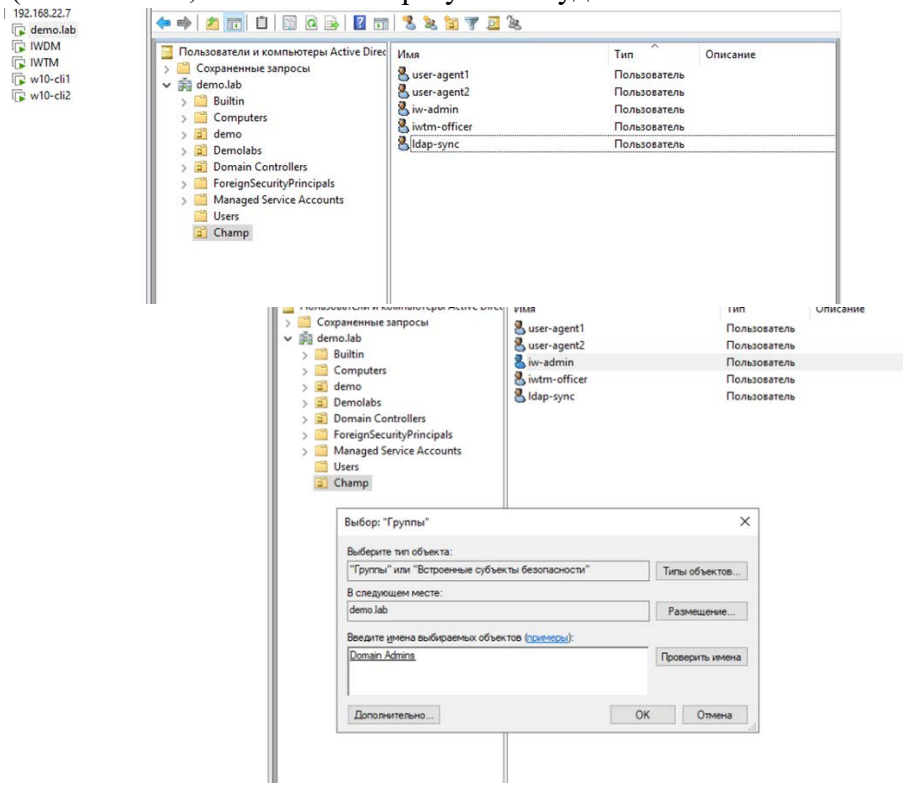
В нашем случае изменяется название подразделение – QualExam (и лучше убрать галочку «Защитить контейнер от случайного удаления)



Далее создаем необходимых пользователей (необходимо заполнить как показано в этом примере «имя» и «имя входа пользователя»

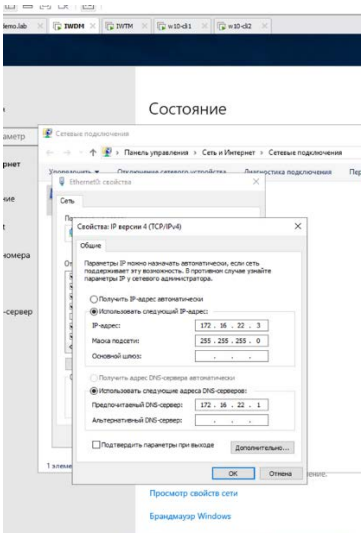


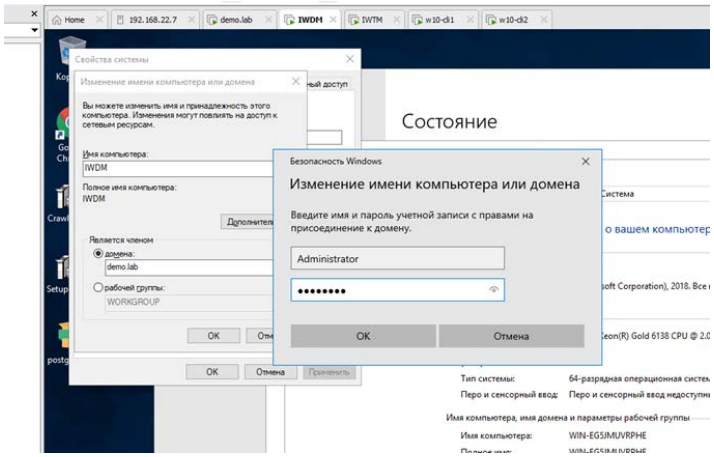
(не забываем, что конечный результат будет отличаться в зависимости от задания)



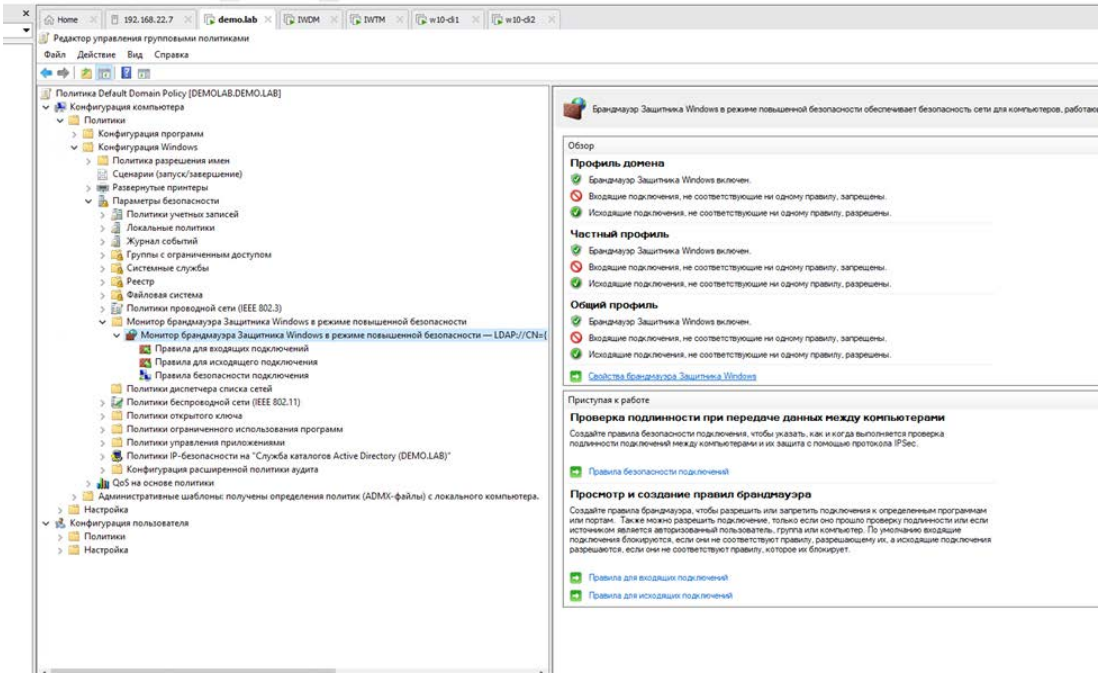
Права администратора для iw-admin (зайти в его свойства> группы)

Далее проверяем сетевые настройки на IWDM.

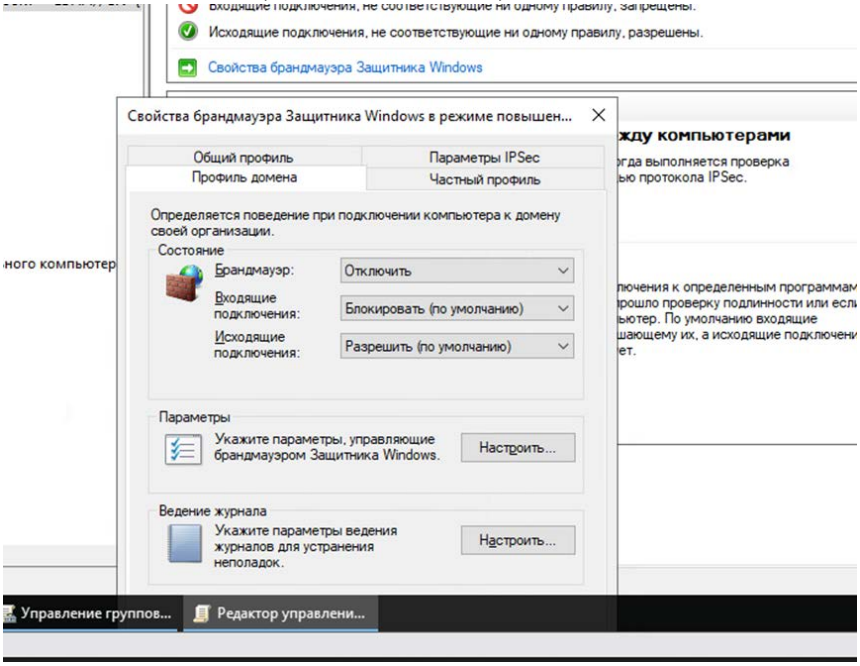




Меняем имя и вносим в домен.

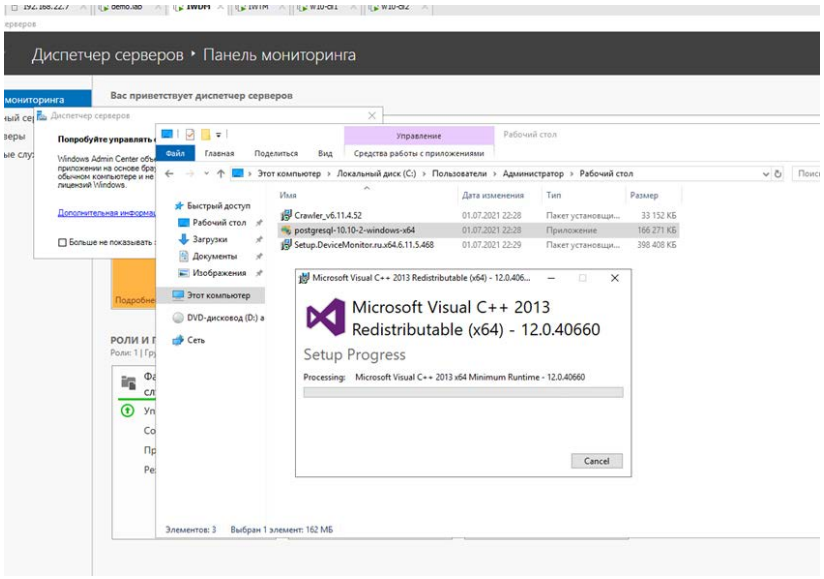


Чтобы сюда попасть нужно нажать правой кнопкой мыши на Default Domain Policy (нажать изменить)



Отключаем брандмауэр

Далее переходим на IWDM – вход от лица ранее созданного пользователя (iw-admin)



(При установке оставляем все без изменения, кроме пароля)

Устанавливаем базу (в случае возникновения ошибки при установке необходимо заново попробовать установить. В случае если появится синий слон – убрать галочку в этом окне).

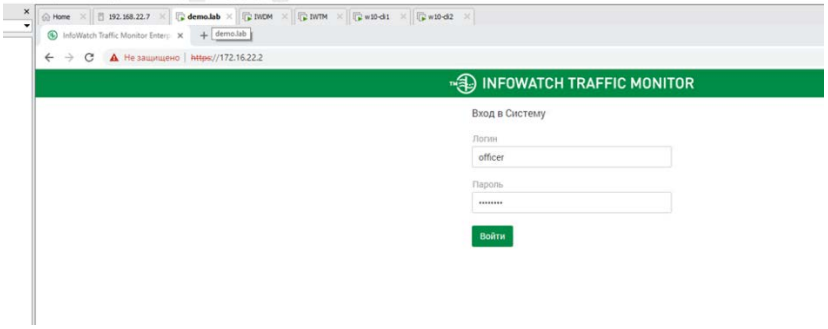
Откройте установщик правой кнопкой мыши от имени админа. Уберите галочку с Stack Bulder, при вводе пароля необходимо убедится, что язык выбран англ.

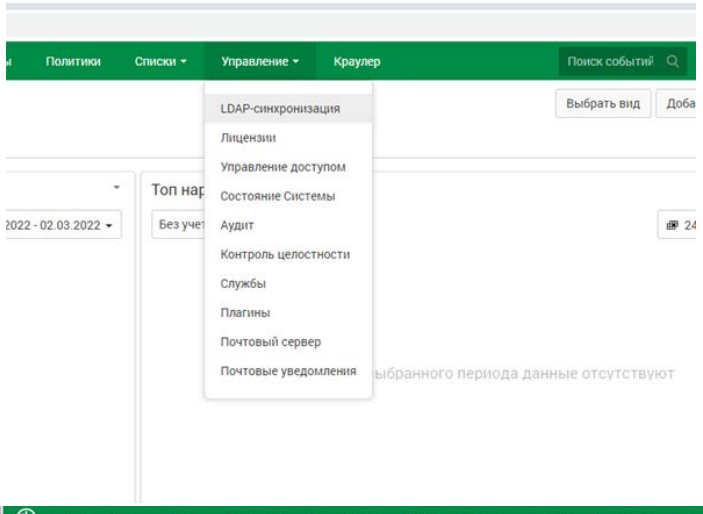
Задание 2: Настройка DLP сервера

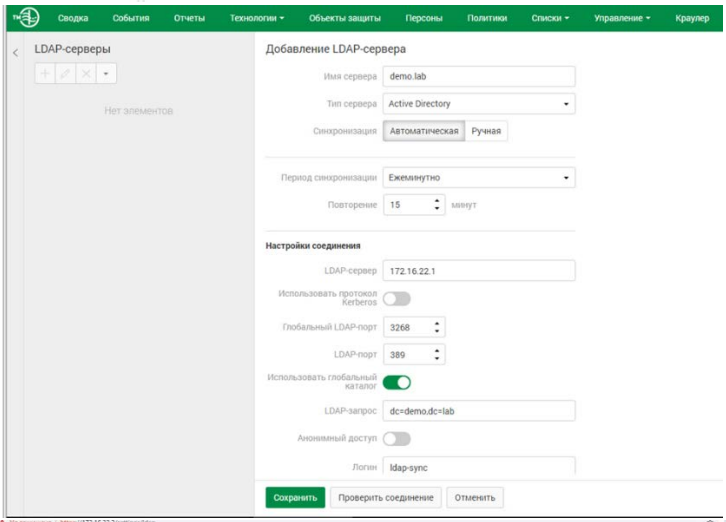
DLP-сервер контроля сетевого трафика уже предустановлен, но не

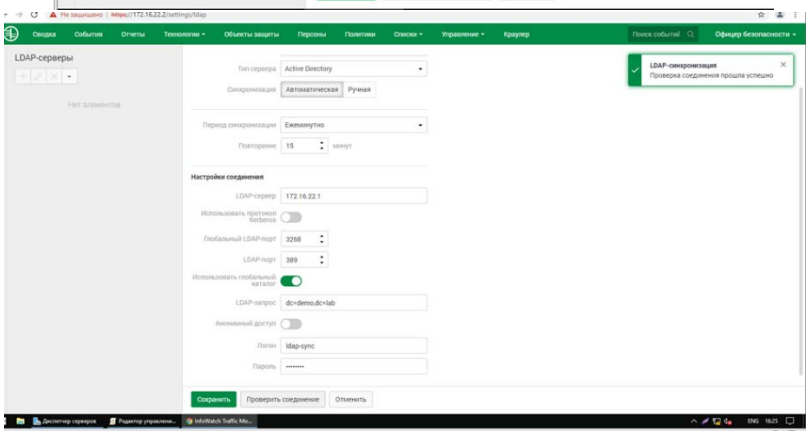
настроен. Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя ldap-sync. Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена iwtm-officer с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

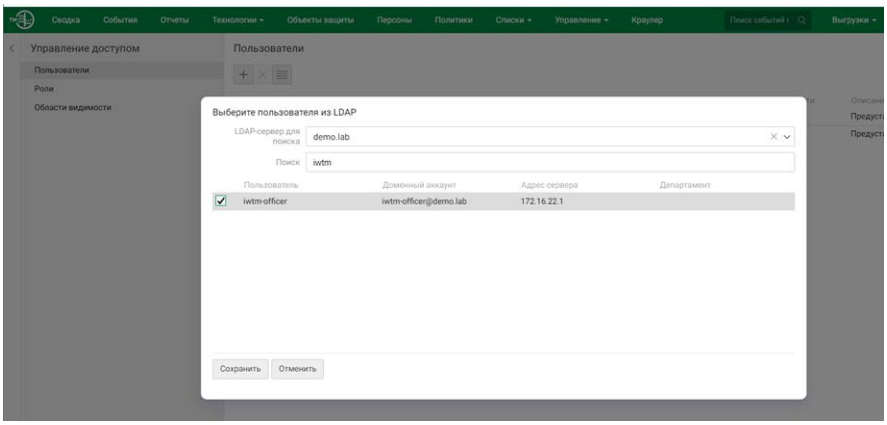
Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» на рабочем столе компьютера.



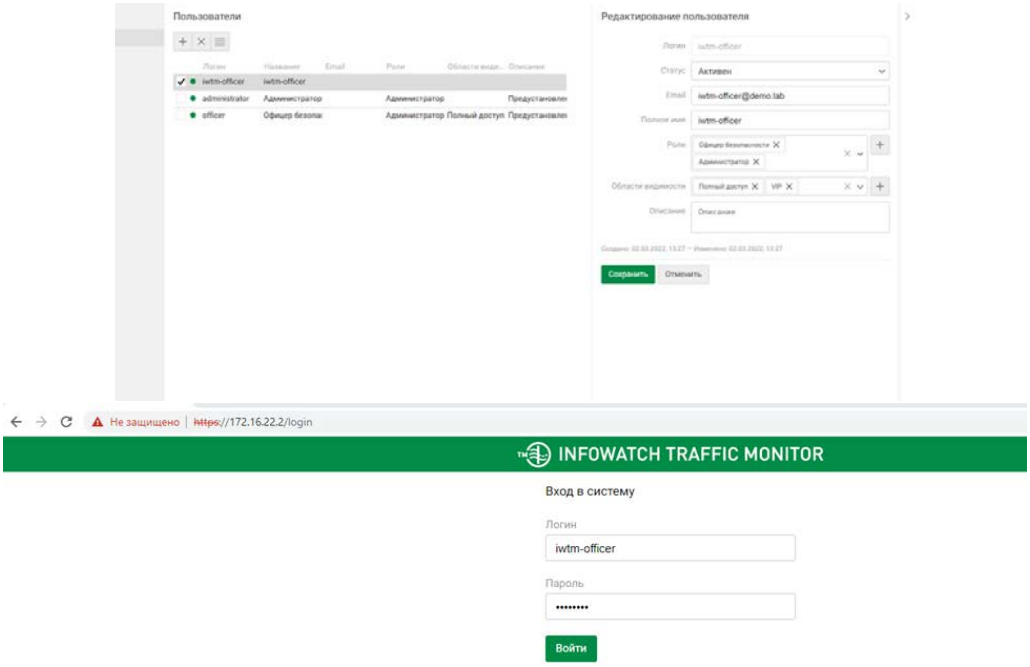








Не выбираем vip.



(Все должно быть также как в обычном офицере)

После этого не забыть создать документ с скриншотами.

Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя iw-admin (важно). После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “QualExam” на домене.

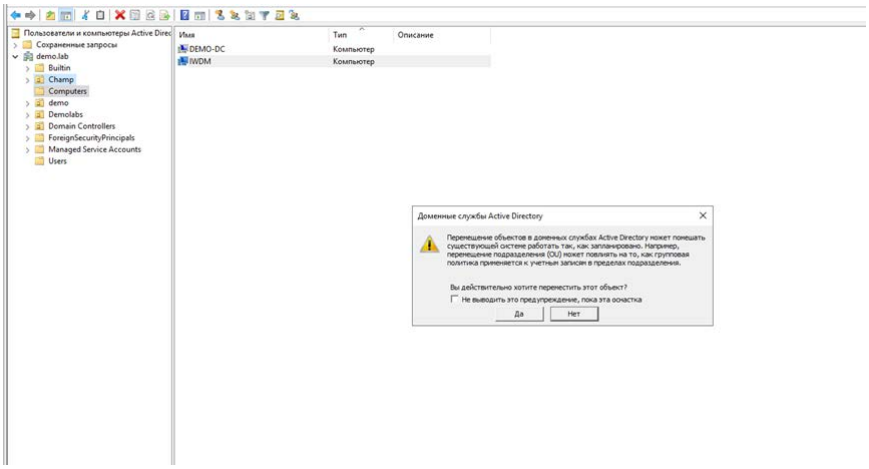
Установить базу данных PostgreSQL с паролем суперпользователя xxXX1234.

Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

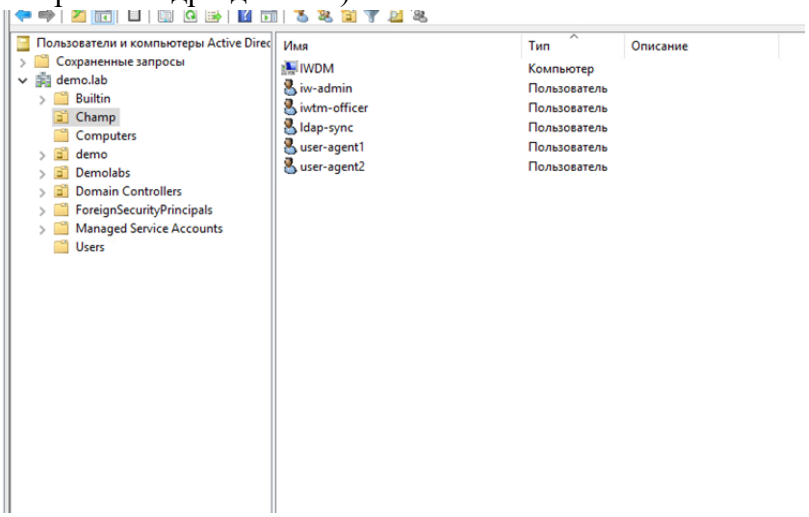
При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: officer с паролем xxXX1234

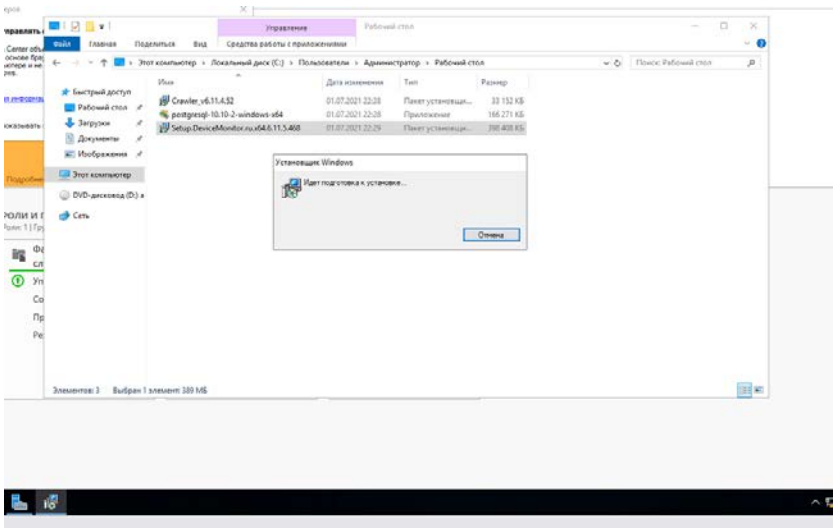
Синхронизировать каталог пользователей и компьютеров с Active Directory. После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя iw-admin, установить полный доступ к системе, установить все области видимости.

Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.

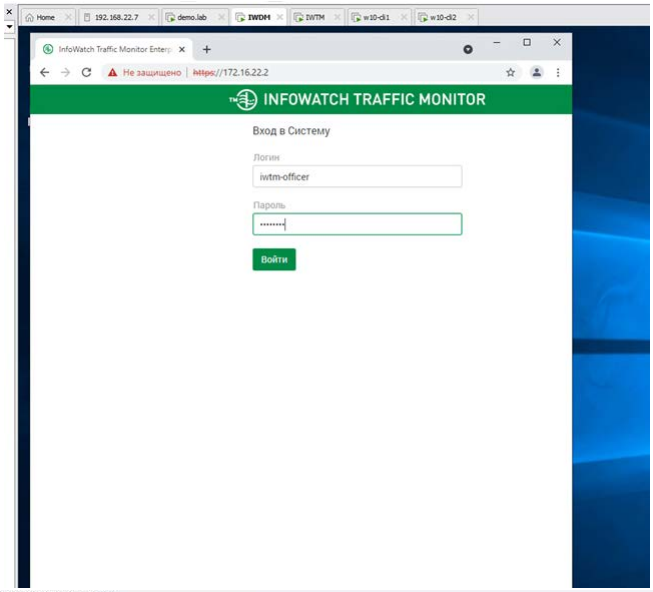


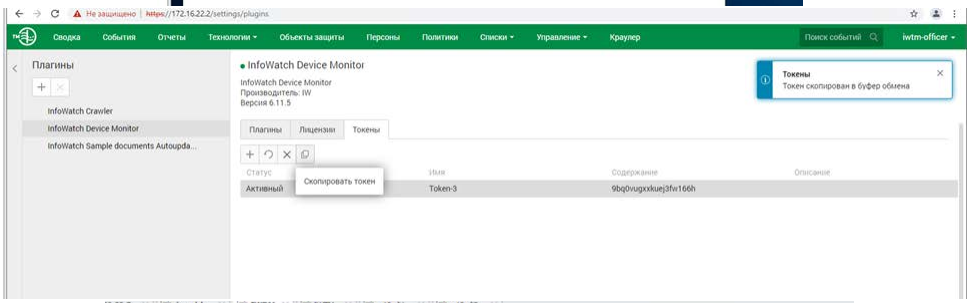
Подразделение будет отличаться, но принцип такой же (перетащить с папки где компьютеры в созданное ранее подразделение)

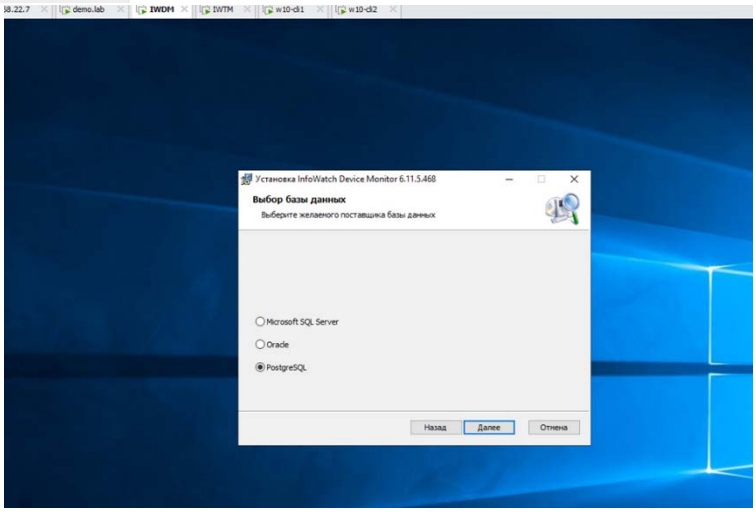


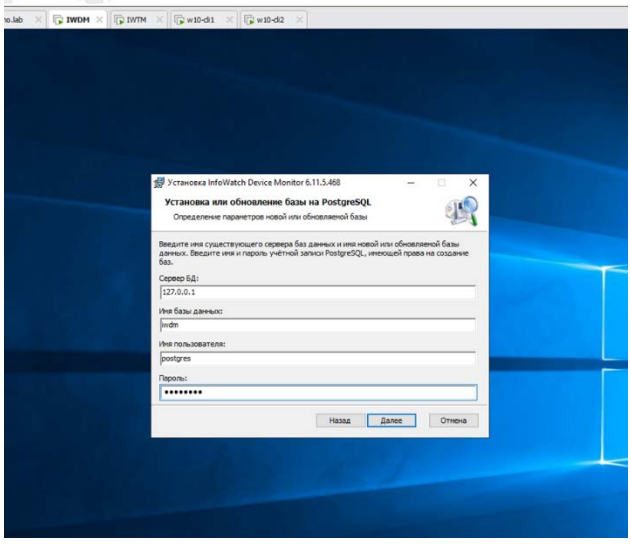


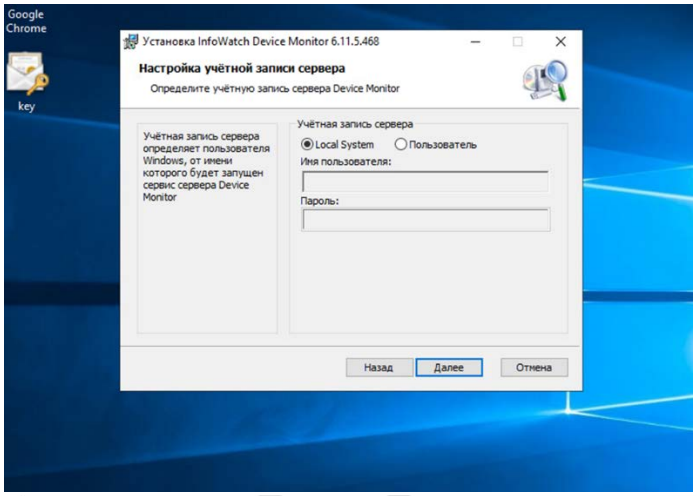
Далее снова переходим на iwdm и начинаем установку (скриншоты только где происходи изменение)

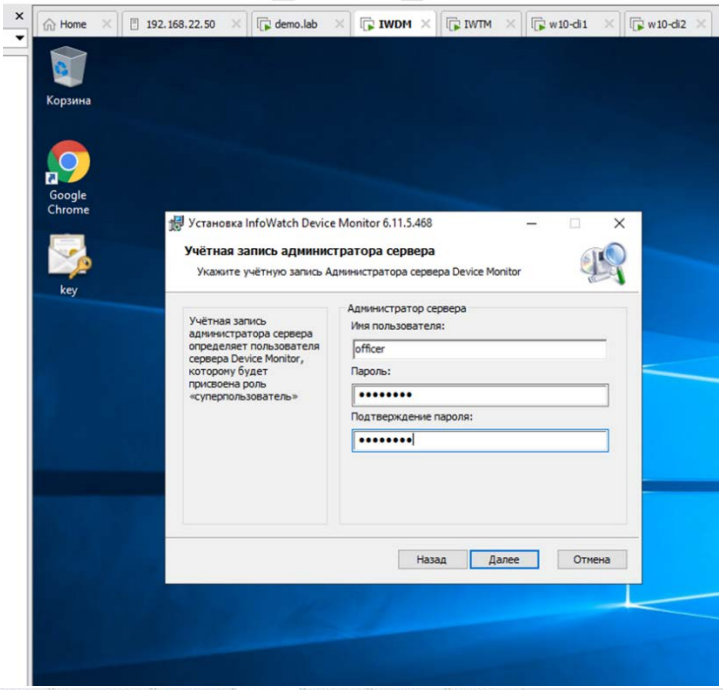

InfoWatch Traffic Monitor Enterp
Не защищено | https://172.16.22.2
INFOWATCH TRAFFIC MONITOR
Вход в Систему
Логин
iwtm-officer
Пароль
Войти

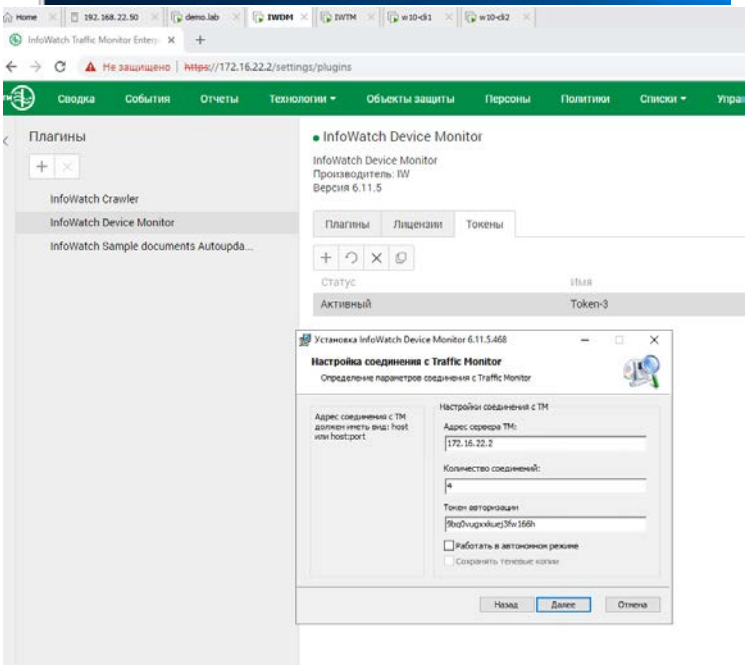

Не защищено | https://172.16.22.2/settings/plugins
Сводка
События
Отчеты
Технологии
Объекты защиты
Персоны
Политики
Списки
Управление
Краулер
Поиск событий
iwtm-officer
Плагины
InfoWatch Crawler
InfoWatch Device Monitor
InfoWatch Sample documents Autoupda...
InfoWatch Device Monitor
InfoWatch Device Monitor
Производитель: IW
Версия 6.11.5
Токены
Токен скопирован в буфер обмена
Плагины
Лицензии
Токены
Статус
Имя
Содержание
Описание
Активный
Скопировать токен
Token-3
9bq0vugxxkuejsfw166h


Установка InfoWatch Device Monitor 6.11.5.468
Выбор базы данных
Выберите желаемого поставщика базы данных
Microsoft SQL Server
Oracle
PostgreSQL
Назад
Далее
Отмена

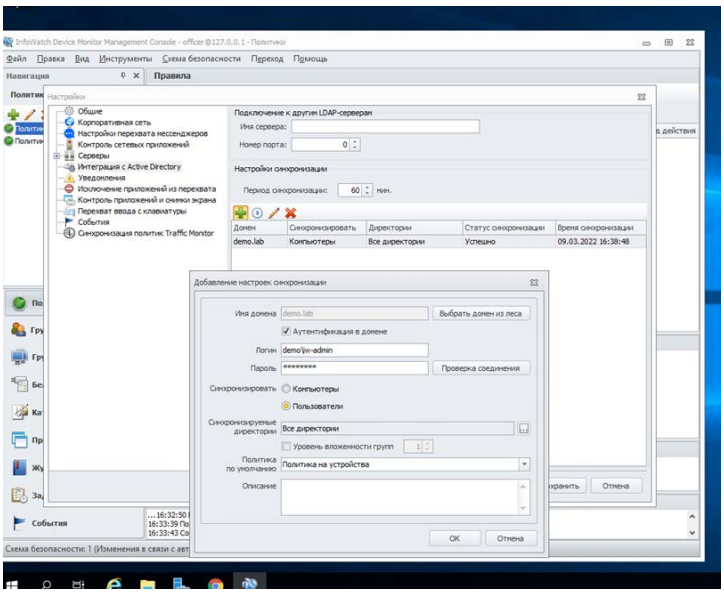

Установка InfoWatch Device Monitor 6.11.5.468
Установка или обновление базы на PostgreSQL
Определение параметров новой или обновляемой базы
Введите имя существующего сервера баз данных и имя новой или обновляемой базы данных. Введите имя и пароль учётной записи PostgreSQL, имеющей права на создание баз.
Сервер БД:
127.0.0.1
Имя базы данных:
iwdm
Имя пользователя:
postgres
Пароль:
Назад
Далее
Отмена



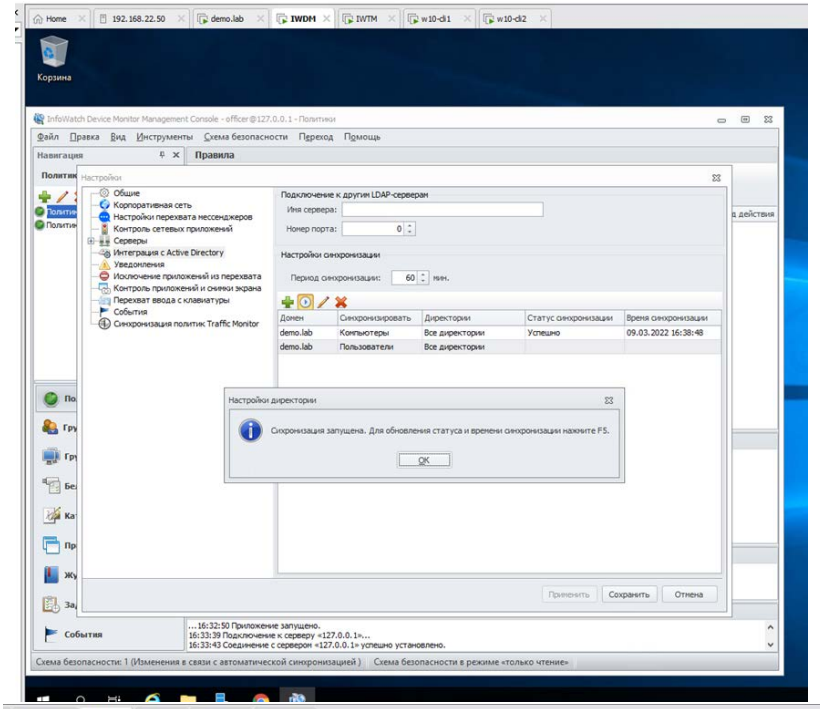


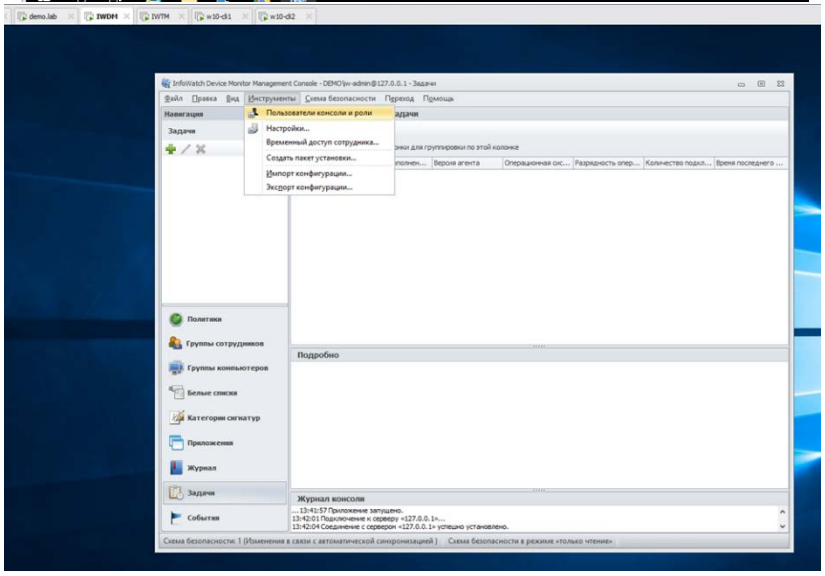


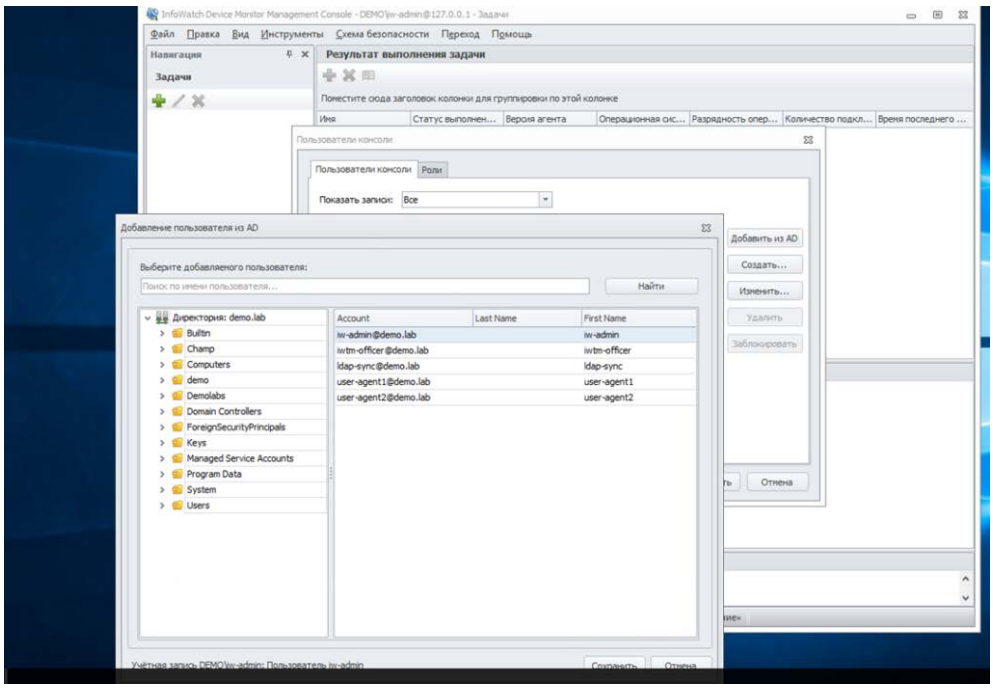
Далее вход в консоль на рабочем столе



Не забыть седлать тоже самое с ПК

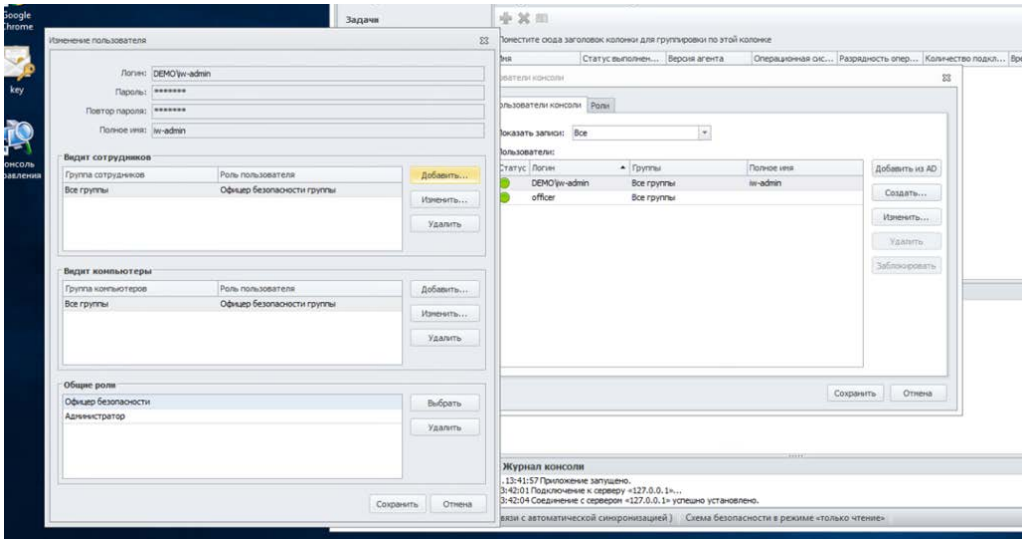




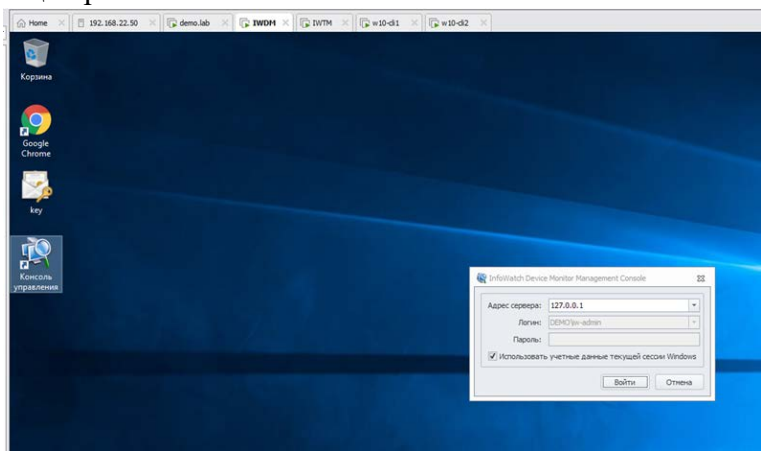


Выбираем добавить из AD

Далее из ранее созданного подразделения – iw-admin и жмем сохранить



Далее выбираем DEMO\iw-admin и жмем изменить, добавляем видит сотрудников, видит компьютеры, общие роли



Теперь проверяем вход без пароля

Задание 4: Установка агента мониторинга на машине нарушителя

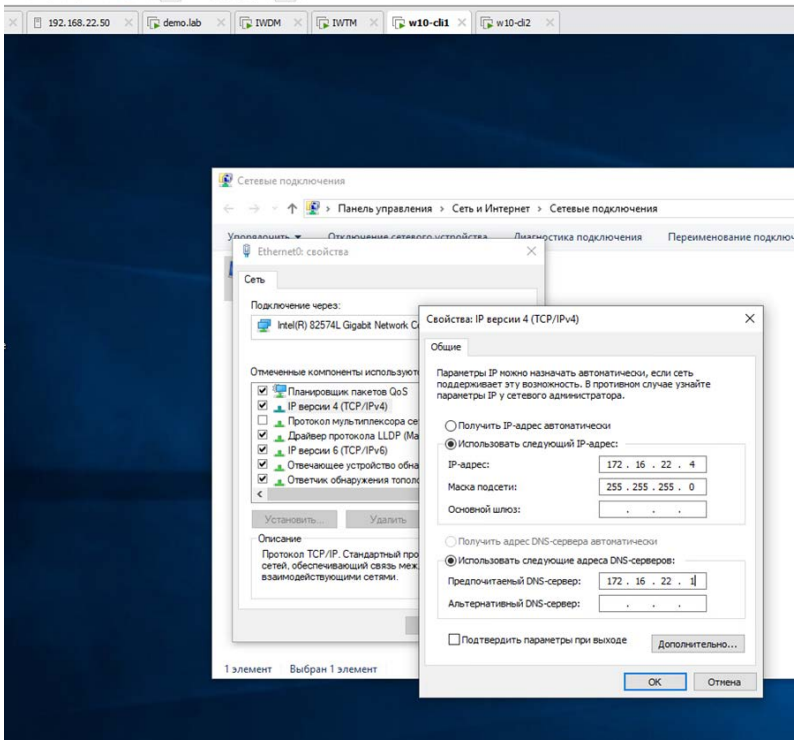
Необходимо ввести клиентскую машину 1 в домен, после перезагрузки войти в систему от ранее созданного пользователя user-agent1.

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя user-agent2.

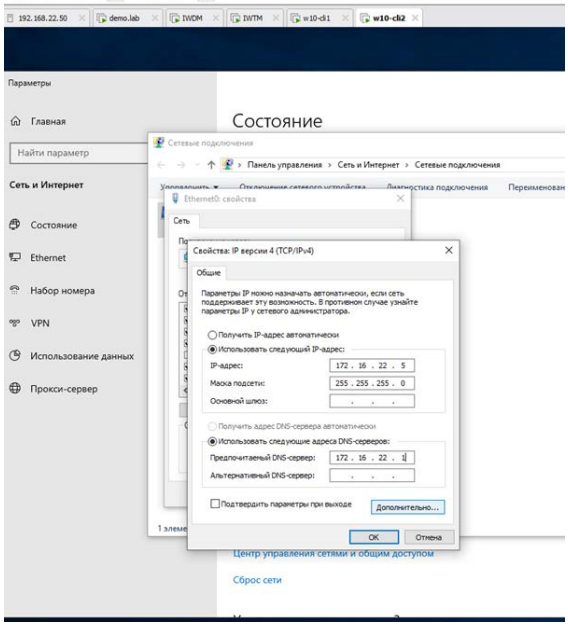
После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение “Champ” на домене.

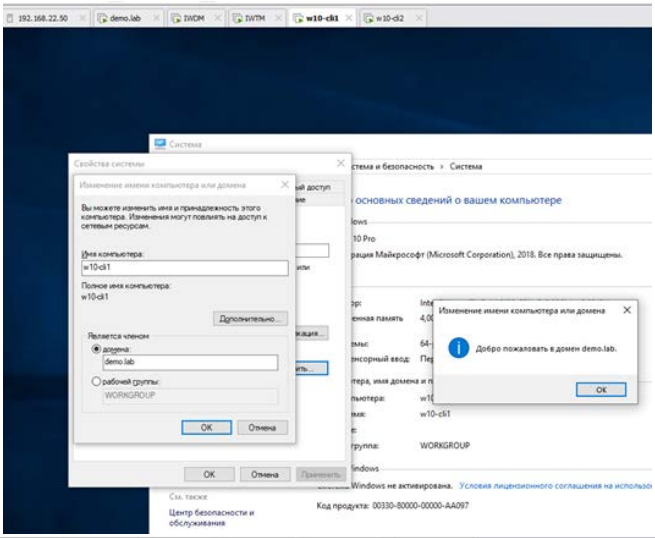
Установить агент мониторинга:

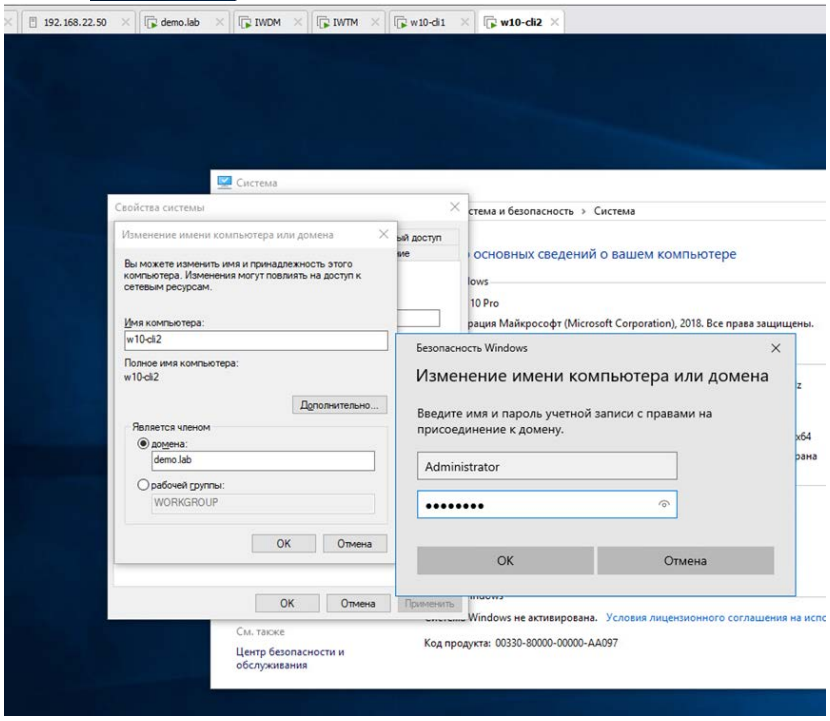
На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга. На машину 2 с помощью групповых политик домена. Необходимо создавать отдельные объекты групповых политик на каждое задание и делать снимки экрана для подтверждения создания и выполнения политик. Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания



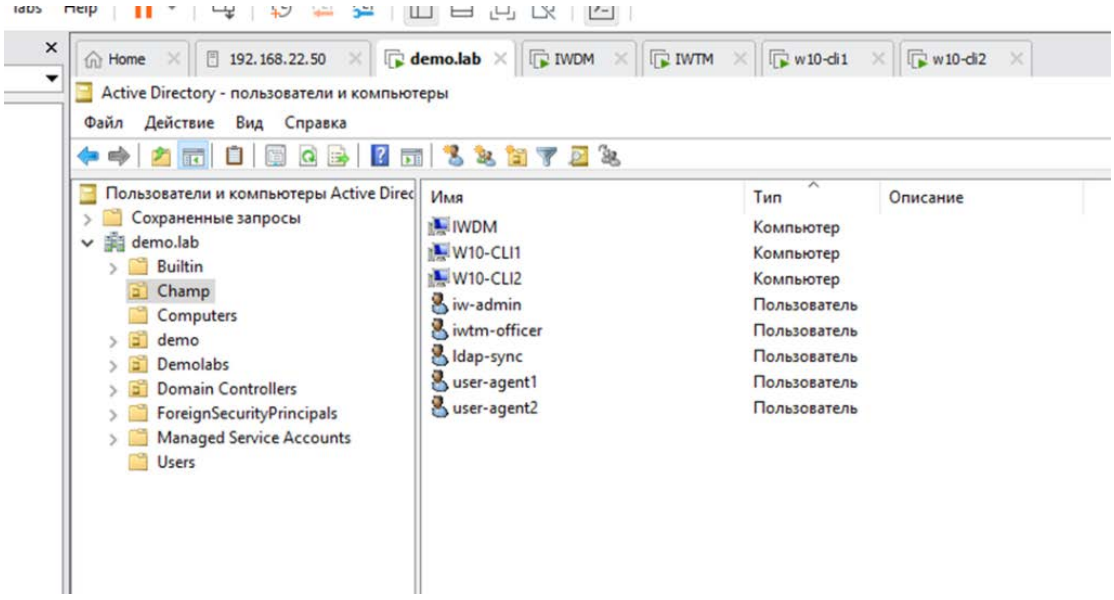
На клиенте проверяем сетевую настройку.



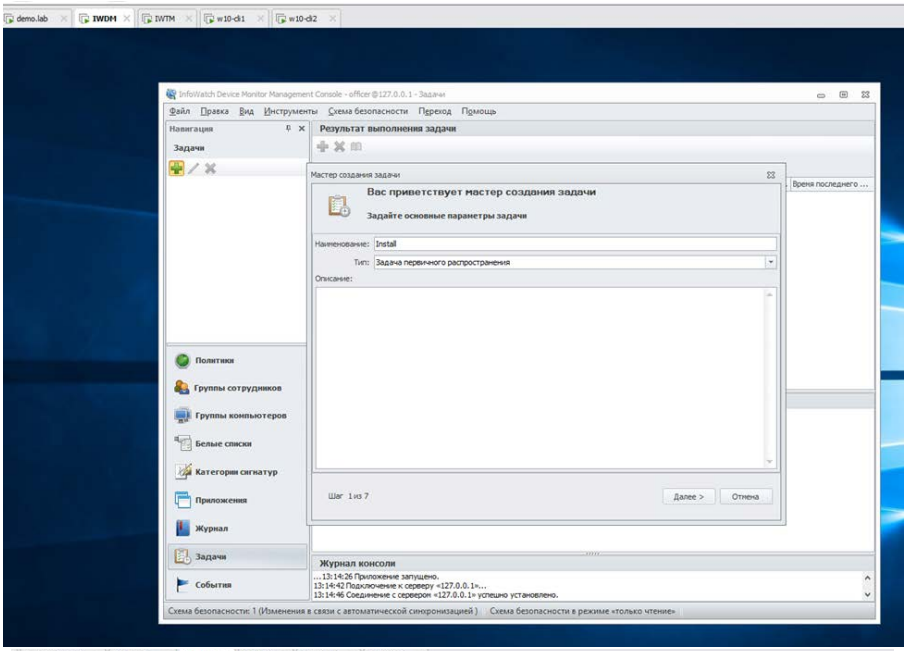


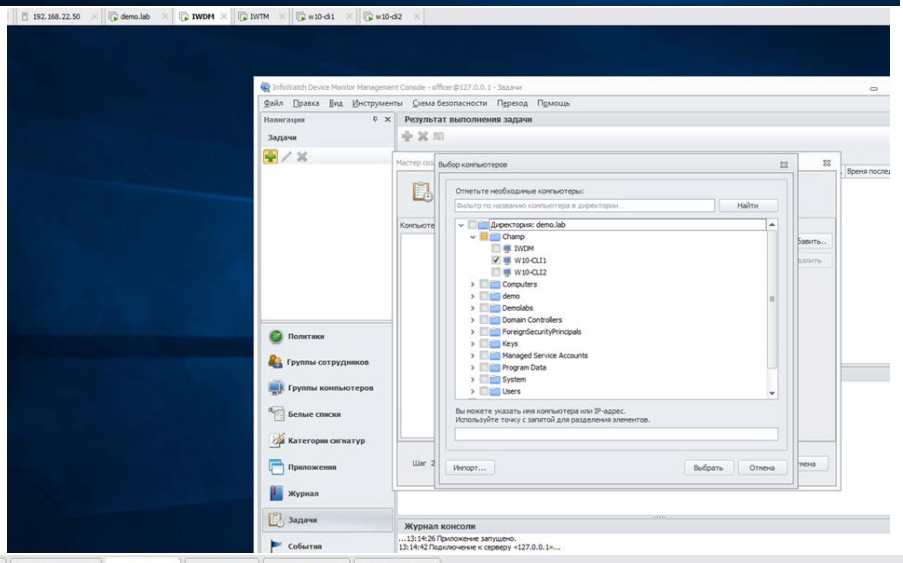


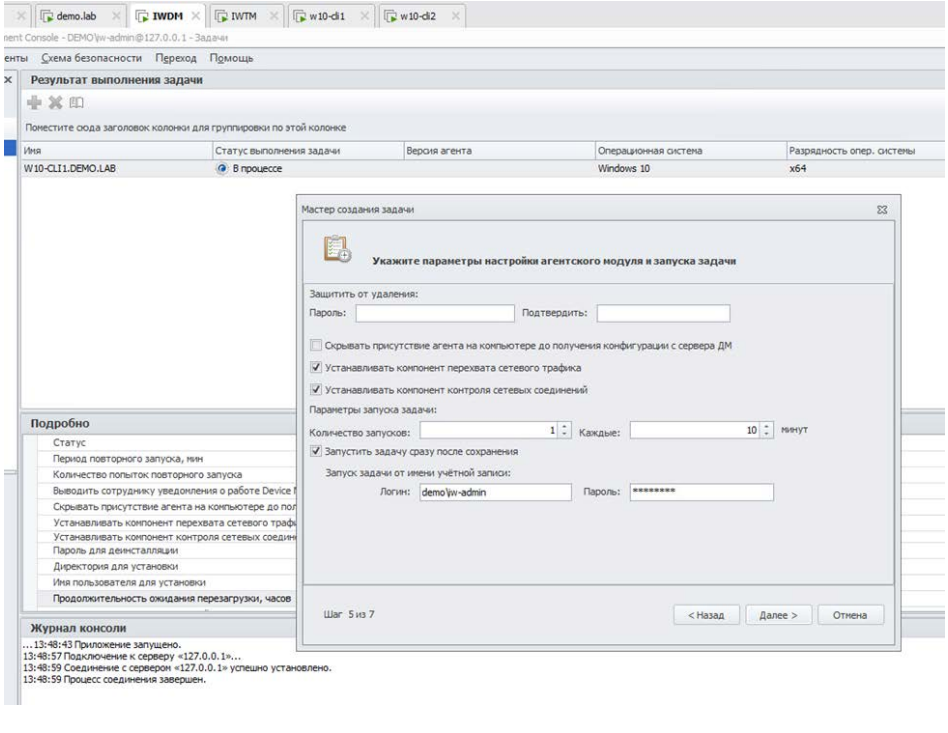
Меняем имя и вносим в домен



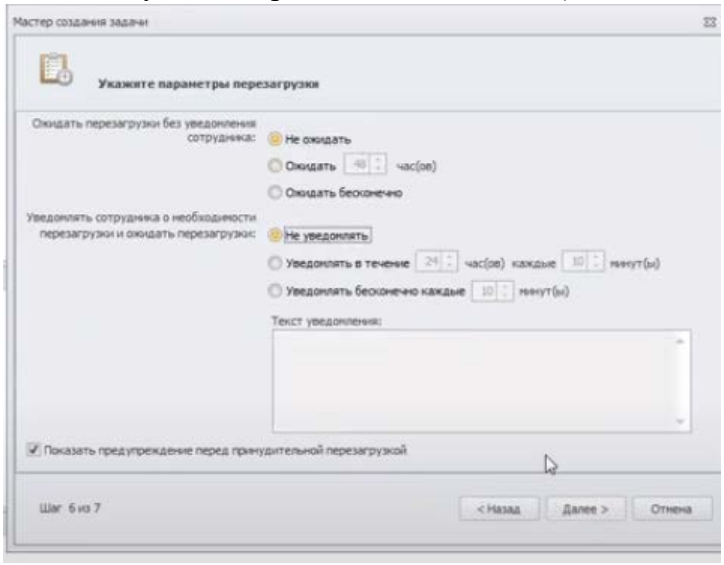
Просто перетаскиваем пк клиента с Computers в подразделение

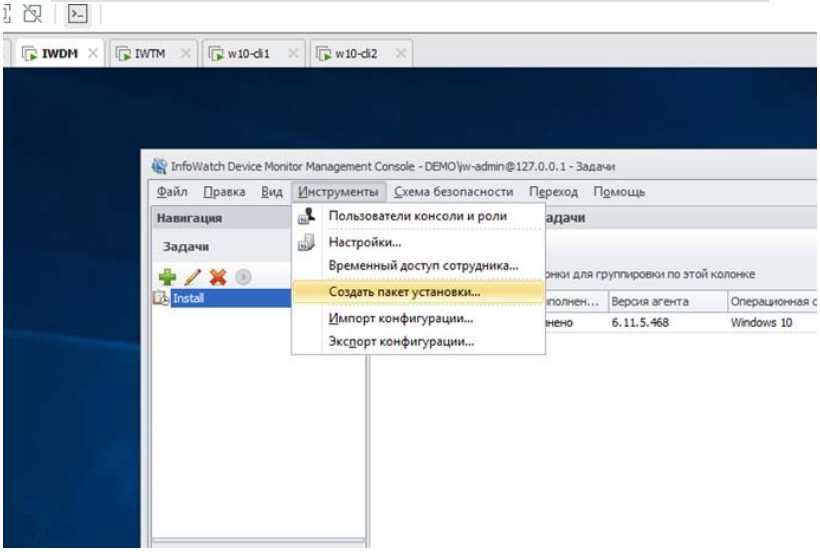

demo.lab
IWDM
IWTM
w10-cli1
w10-cli2
Файл Правка Вид Инструменты Схема безопасности Переход Помощь
Навигация
Задачи
Результат выполнения задачи
Мастер создания задачи
Вас приветствует мастер создания задачи
Задайте основные параметры задачи
Наименование: Install
Тип: Задача первичного распространения
Описание:
Шаг 1 из 7
Далее >
Отмена
Политики
Группы сотрудников
Группы компьютеров
Белые списки
Категории сигнатур
Приложения
Журнал
Задачи
События
Журнал консоли
...13:14:26 Приложение запущено.
13:14:42 Подключение к серверу «127.0.0.1»...
13:14:46 Соединение с сервером «127.0.0.1» успешно установлено.

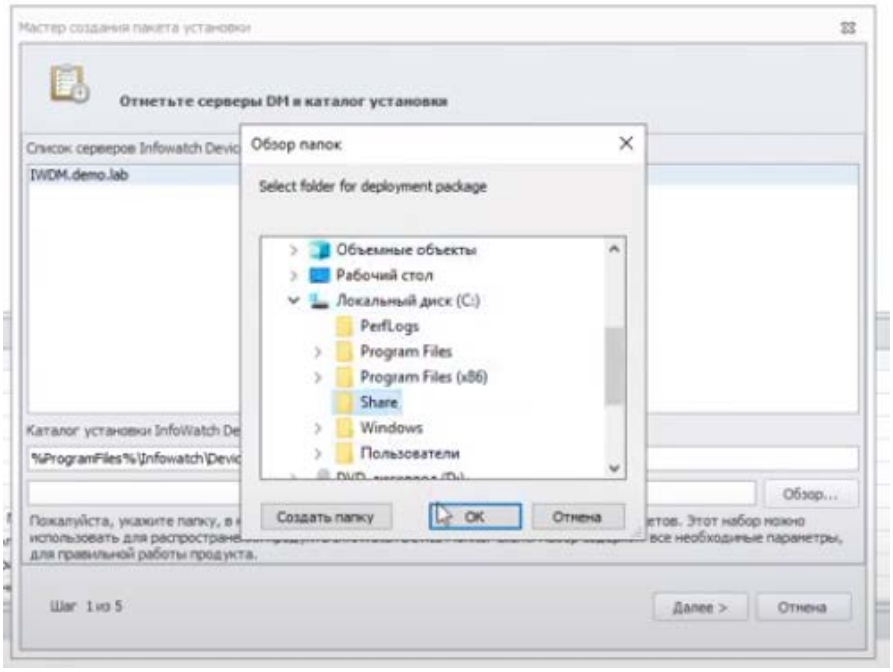

192.168.22.50
demo.lab
IWDM
IWTM
w10-cli1
w10-cli2
Выбор компьютеров
Отметьте необходимые компьютеры:
Найти
Директория: demo.lab
Champ
IWDM
W10-CLI1
W10-CLI2
Computers
demo
Demolabs
Domain Controllers
ForeignSecurityPrincipals
Keys
Managed Service Accounts
Program Data
System
Users
Импорт...
Выбрать
Отмена

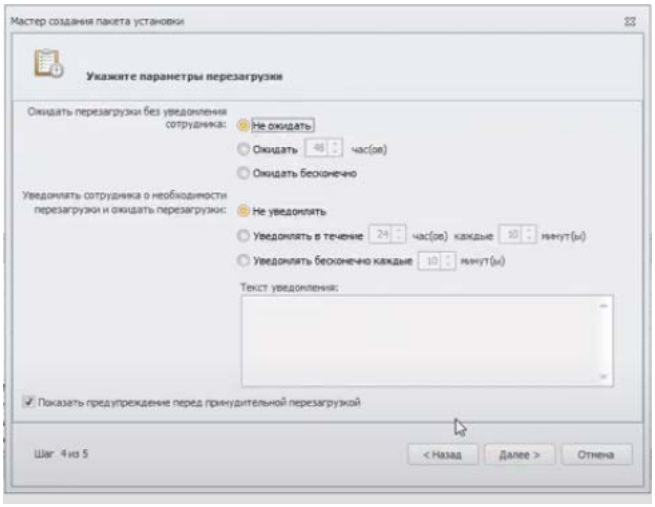

demo.lab
IWDM
IWTM
w10-cli1
w10-cli2
Результат выполнения задачи
Поместите сюда заголовок колонки для группировки по этой колонке
Имя
Статус выполнения задачи
Версия агента
Операционная система
Разрядность опер. системы
W10-CLI1.DEMO.LAB
В процессе
Windows 10
x64
Мастер создания задачи
Укажите параметры настройки агентского модуля и запуска задачи
Защитить от удаления:
Пароль:
Подтвердить:
Скрывать присутствие агента на компьютере до получения конфигурации с сервера ДМ
Устанавливать компонент перехвата сетевого трафика
Устанавливать компонент контроля сетевых соединений
Параметры запуска задачи:
Количество запусков: 1
Каждые: 10
минут
Запустить задачу сразу после сохранения
Запуск задачи от имени учётной записи:
Логин: demo\jw-admin
Пароль: ********
Шаг 5 из 7
< Назад
Далее >
Отмена
Подробно
Статус
Период повторного запуска, мин
Количество попыток повторного запуска
Скрывать присутствие агента на компьютере до пол
Устанавливать компонент перехвата сетевого трафи
Устанавливать компонент контроля сетевых соедин
Пароль для деинсталляции
Директория для установки
Имя пользователя для установки
Продолжительность ожидания перезагрузки, часов
Журнал консоли
...13:48:43 Приложение запущено.
13:48:57 Подключение к серверу «127.0.0.1»...
13:48:59 Соединение с сервером «127.0.0.1» успешно установлено.
13:48:59 Процесс соединения завершен.

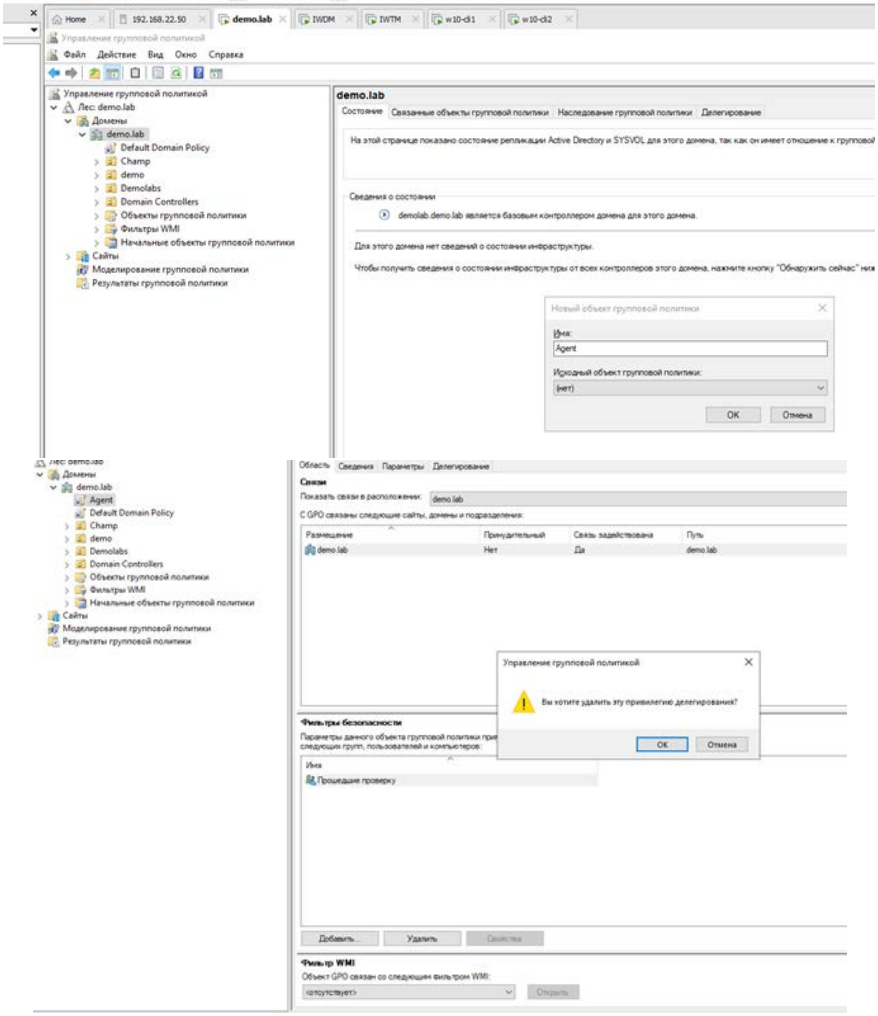
Далее запускаем созданную задачу (после завершения нужно перезагрузить пк и проверить на клиенте агента – сделать скрины установки и результата на агенте – загрузить их в созданный документ на рабочем столе iwdm (создать самому!)



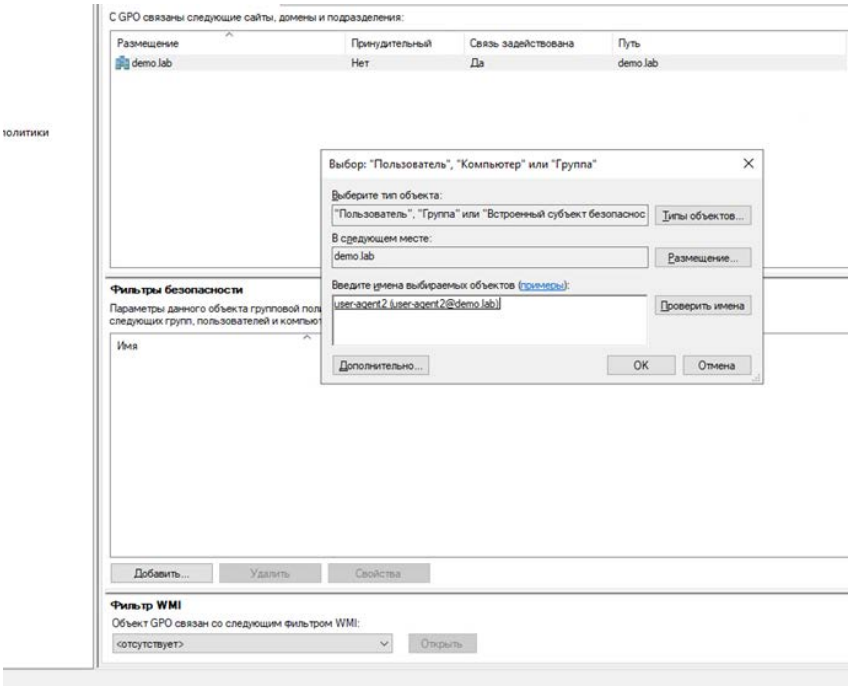




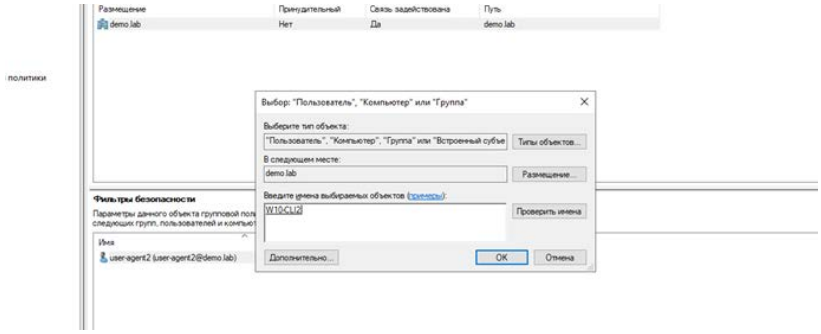




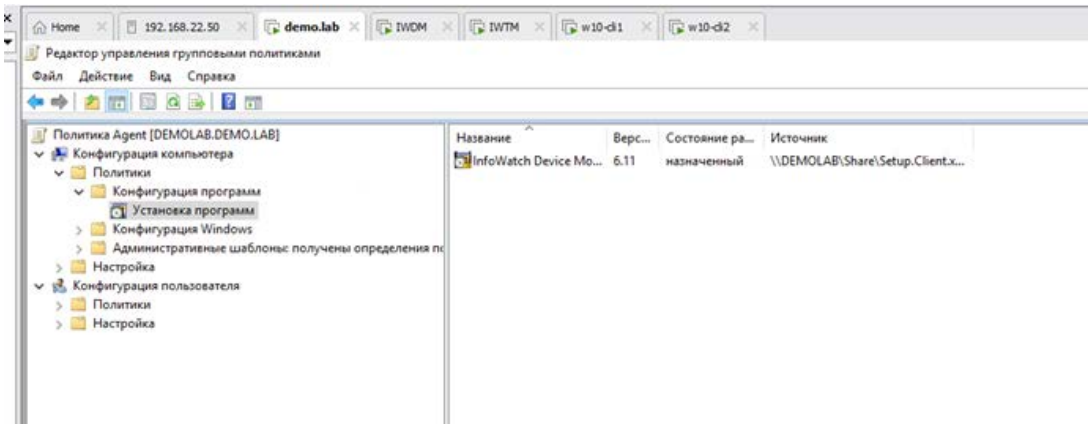
(Удалить – фильтр безопасности)



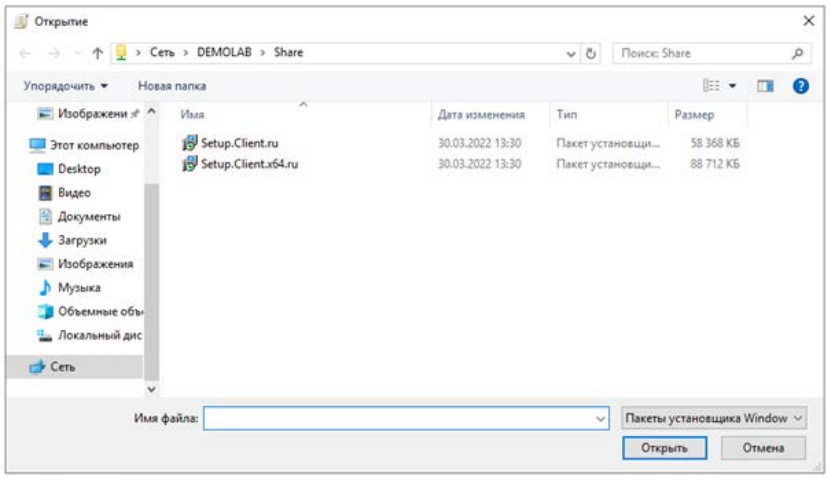
(добавить)



Убедится, что в типах объекта добавлены компьютеры

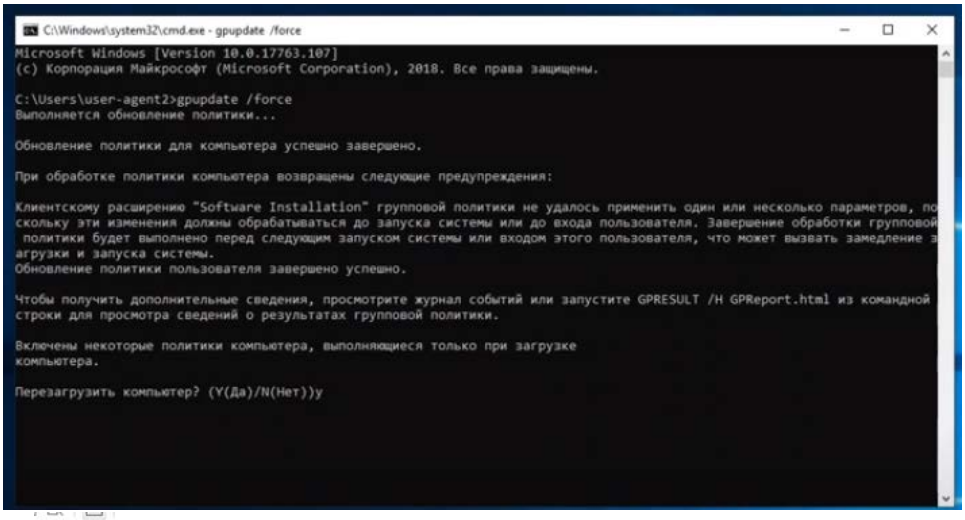


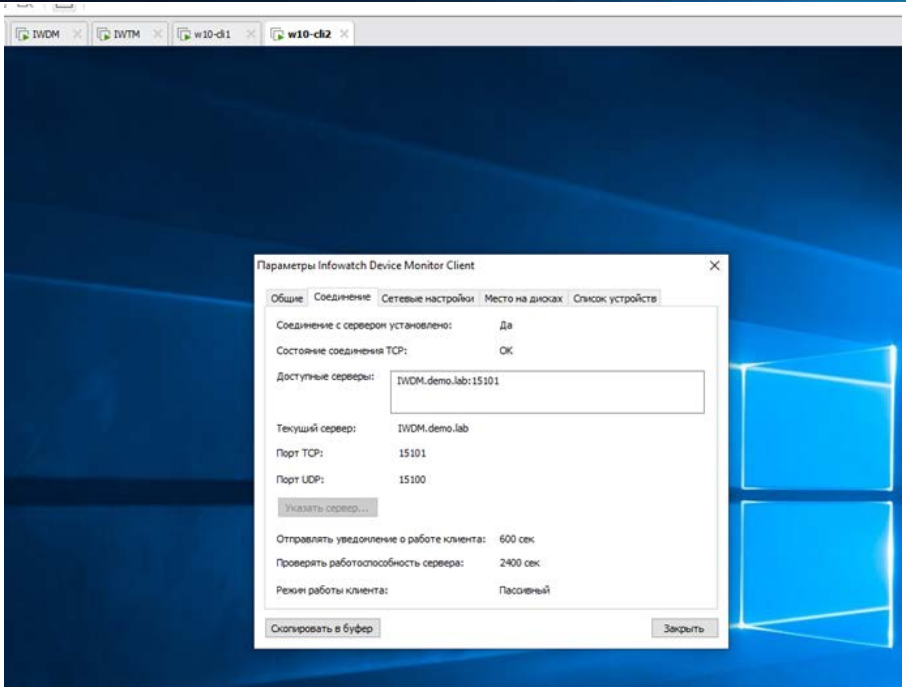
Необходимо создать пакет (нажатие правой кнопки мыши)



Выбрать второй (x64)

Необходимо зайти на 2 машину клиента и зайти в командную строку.

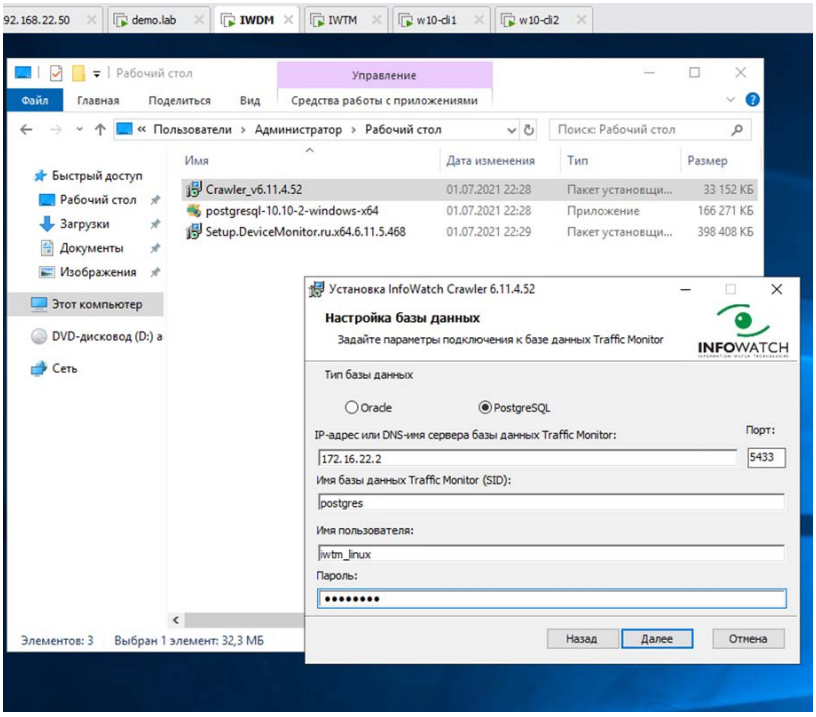




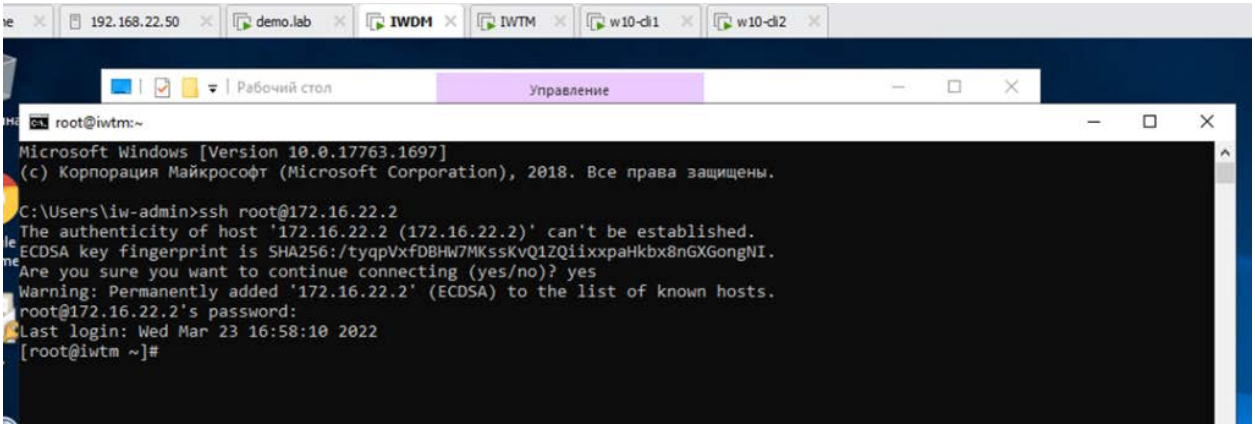
Доложен появится агент

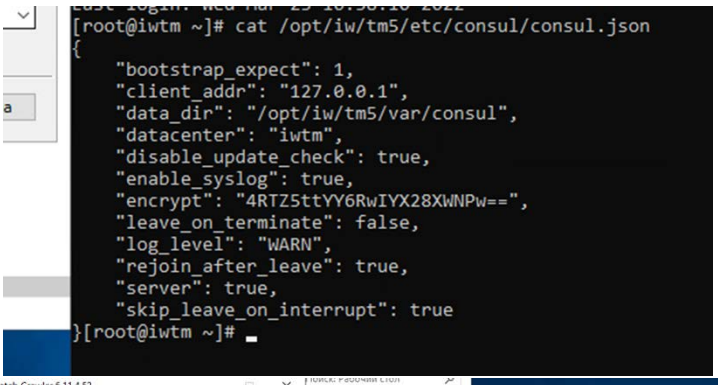
Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов.

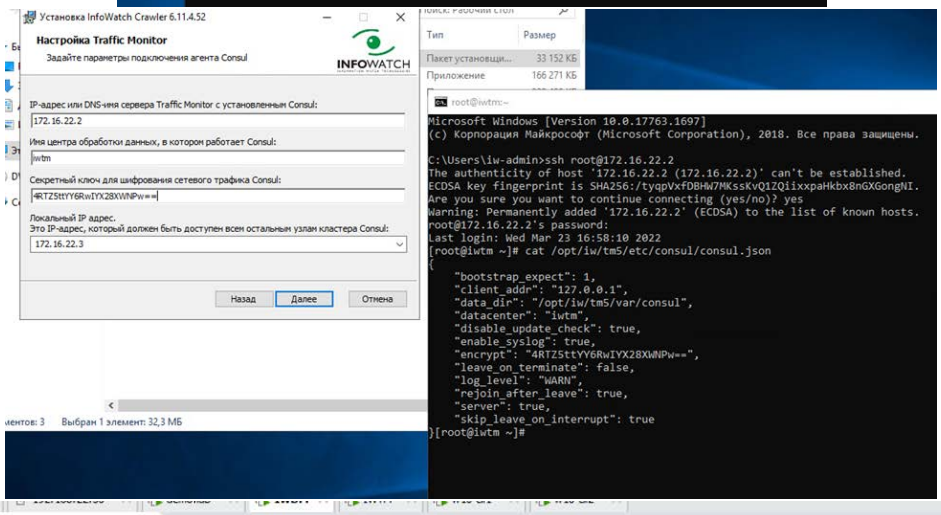
Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга с настройками по умолчанию. Необходимо создать общий каталог Share в корне диска сервера IWDM и установить права доступа на запись и чтение для всех пользователей домена. Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. Для работы подсистемы может потребоваться редактирования конфигурационных файлов (для устранения предупреждения).

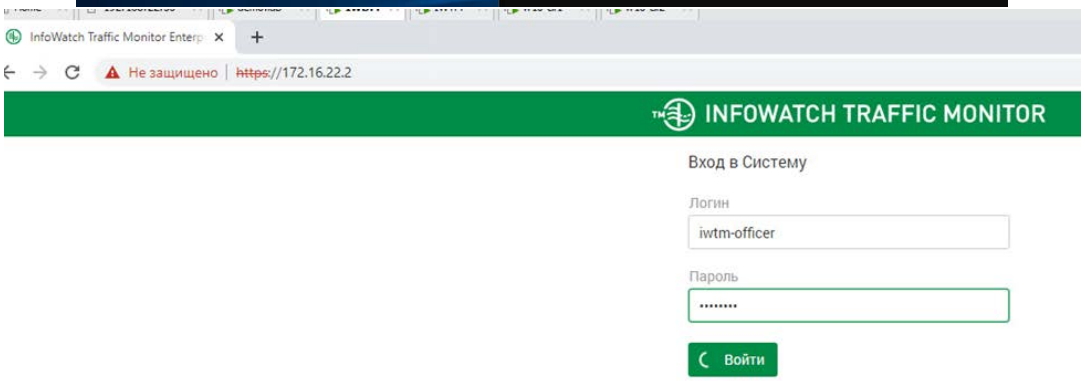


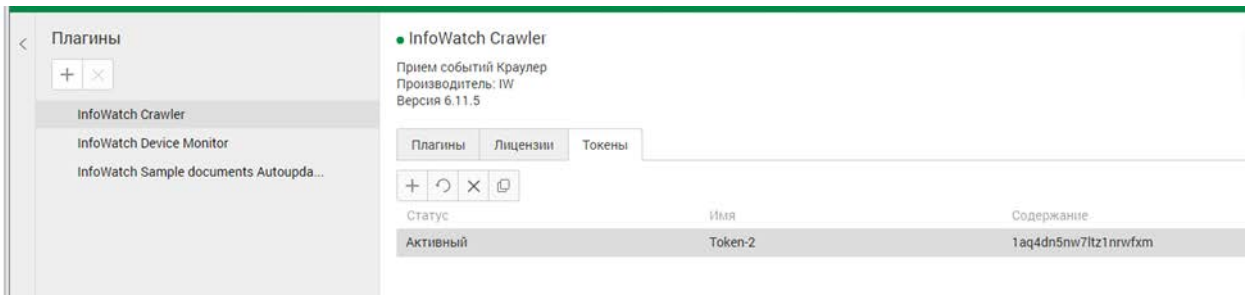
Далее с iwdm необходимо зайти в командную строку для получения информации о Consul

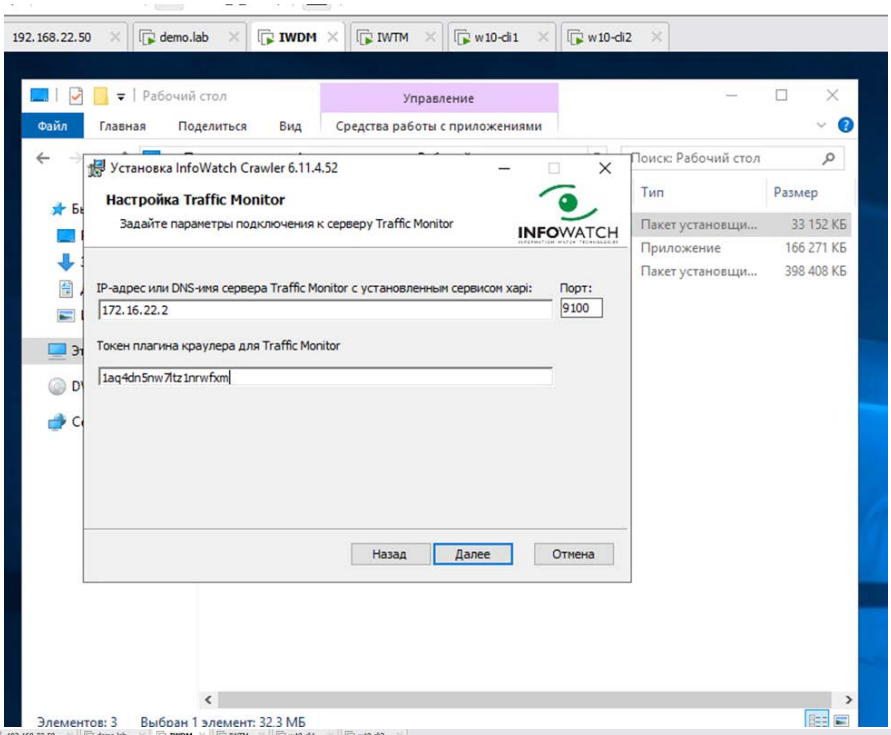


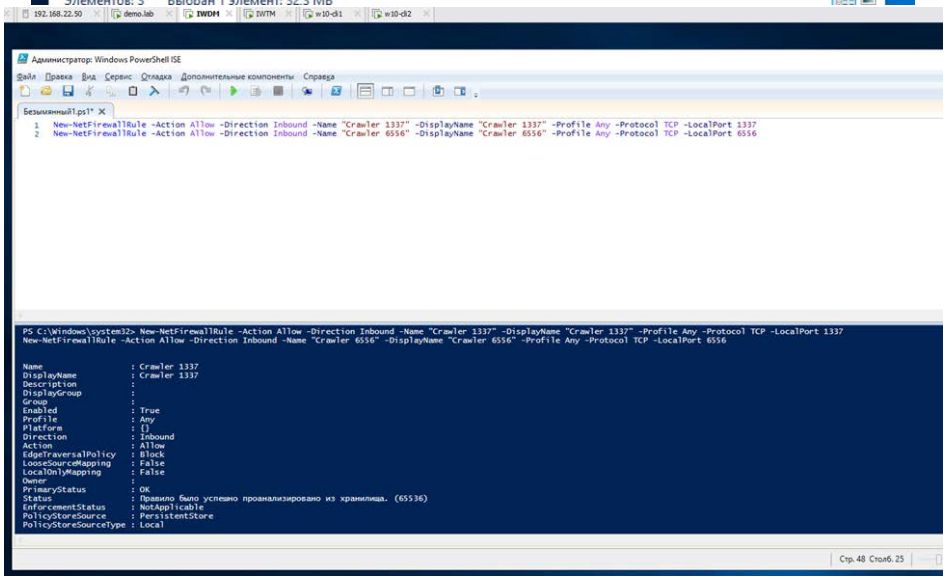

[root@iwtm ~]# cat /opt/iw/tm5/etc/consul/consul.json
{
"bootstrap_expect": 1,
"client_addr": "127.0.0.1",
"data_dir": "/opt/iw/tm5/var/consul",
"datacenter": "iwtm",
"disable_update_check": true,
"enable_syslog": true,
"encrypt": "4RTZ5ttYY6RwIYX28XWNPw==",
"leave_on_terminate": false,
"log_level": "WARN",
"rejoin_after_leave": true,
"server": true,
"skip_leave_on_interrupt": true
}[root@iwtm ~]#


Установка InfoWatch Crawler 6.11.4.52
Настройка Traffic Monitor
Задайте параметры подключения агента Consul
INFOWATCH
IP-адрес или DNS-имя сервера Traffic Monitor с установленным Consul:
172.16.22.2
Имя центра обработки данных, в котором работает Consul:
iwtm
Секретный ключ для шифрования сетевого трафика Consul:
4RTZ5ttYY6RwIYX28XWNPw==
Локальный IP адрес.
Это IP-адрес, который должен быть доступен всем остальным узлам кластера Consul:
172.16.22.3
Назад
Далее
Отмена
Тип
Размер
Пакет установщи...
33 152 КБ
Приложение
166 271 КБ
Microsoft Windows [Version 10.0.17763.1697]
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.
C:\Users\iw-admin>ssh root@172.16.22.2
The authenticity of host '172.16.22.2 (172.16.22.2)' can't be established.
ECDSA key fingerprint is SHA256:/tyqpVxfDBHW7MKssKvQ1ZQiixxpaHkbx8nGXGongNI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.22.2' (ECDSA) to the list of known hosts.
root@172.16.22.2's password:
Last login: Wed Mar 23 16:58:10 2022
[root@iwtm ~]# cat /opt/iw/tm5/etc/consul/consul.json
{
"bootstrap_expect": 1,
"client_addr": "127.0.0.1",
"data_dir": "/opt/iw/tm5/var/consul",
"datacenter": "iwtm",
"disable_update_check": true,
"enable_syslog": true,
"encrypt": "4RTZ5ttYY6RwIYX28XWNPw==",
"leave_on_terminate": false,
"log_level": "WARN",
"rejoin_after_leave": true,
"server": true,
"skip_leave_on_interrupt": true
}[root@iwtm ~]#
Выбран 1 элемент: 32,3 МБ


InfoWatch Traffic Monitor Enterp
Не защищено
https://172.16.22.2
INFOWATCH TRAFFIC MONITOR
Вход в Систему
Логин
iwtm-officer
Пароль
Войти


Плагины
InfoWatch Crawler
InfoWatch Device Monitor
InfoWatch Sample documents Autoupda...
InfoWatch Crawler
Прием событий Краулер
Производитель: IW
Версия 6.11.5
Плагины
Лицензии
Токены
Статус
Имя
Содержание
Активный
Token-2
1aq4dn5nw7ltz1nrwfxm



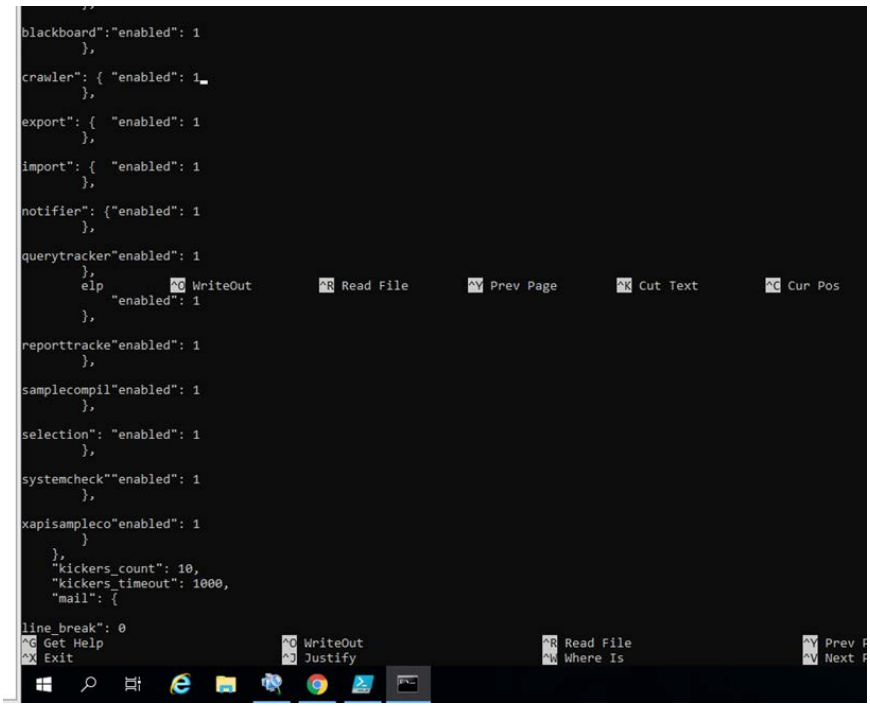


New-NetFirewallRule –Action Allow –Direction Inbound –Name “Crawler 1337” –DisplayName “Crawler 1337” –Profile Any –Protocol TCP –LocalPort 1337

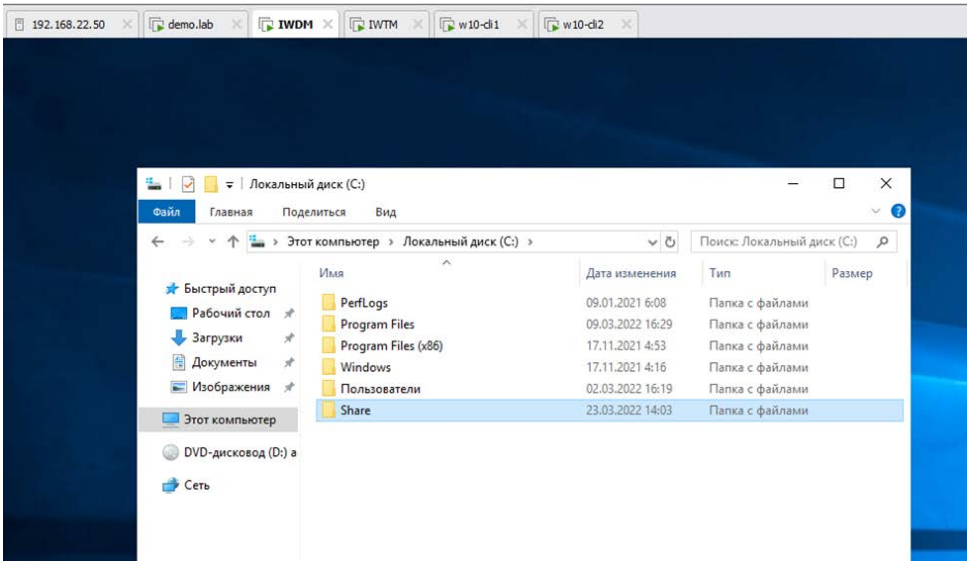
New-NetFirewallRule –Action Allow –Direction Inbound –Name “Crawler 6556” –DisplayName “Crawler 6556” –Profile Any –Protocol TCP –LocalPort 6556

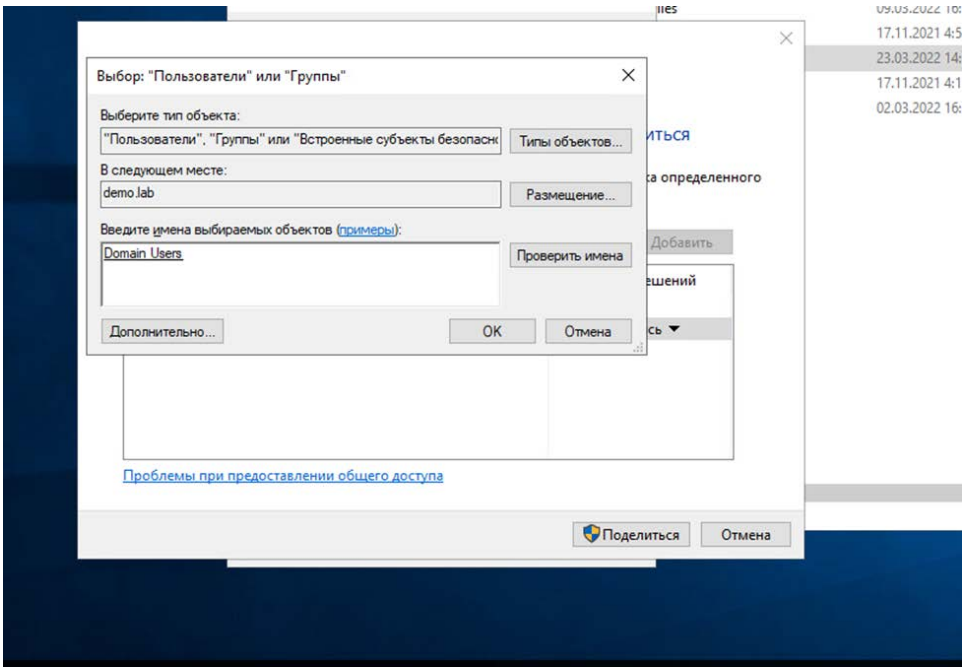
(Необходимо открыть от имени администратора)

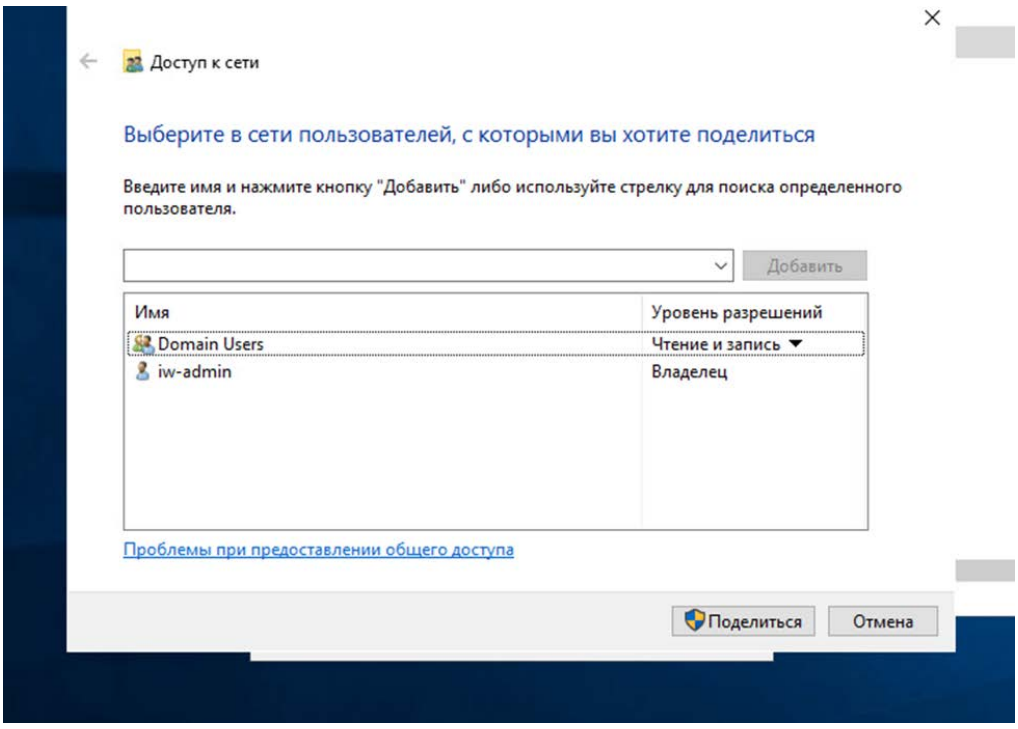
(зайти на iwtm с iwdm (ssh))

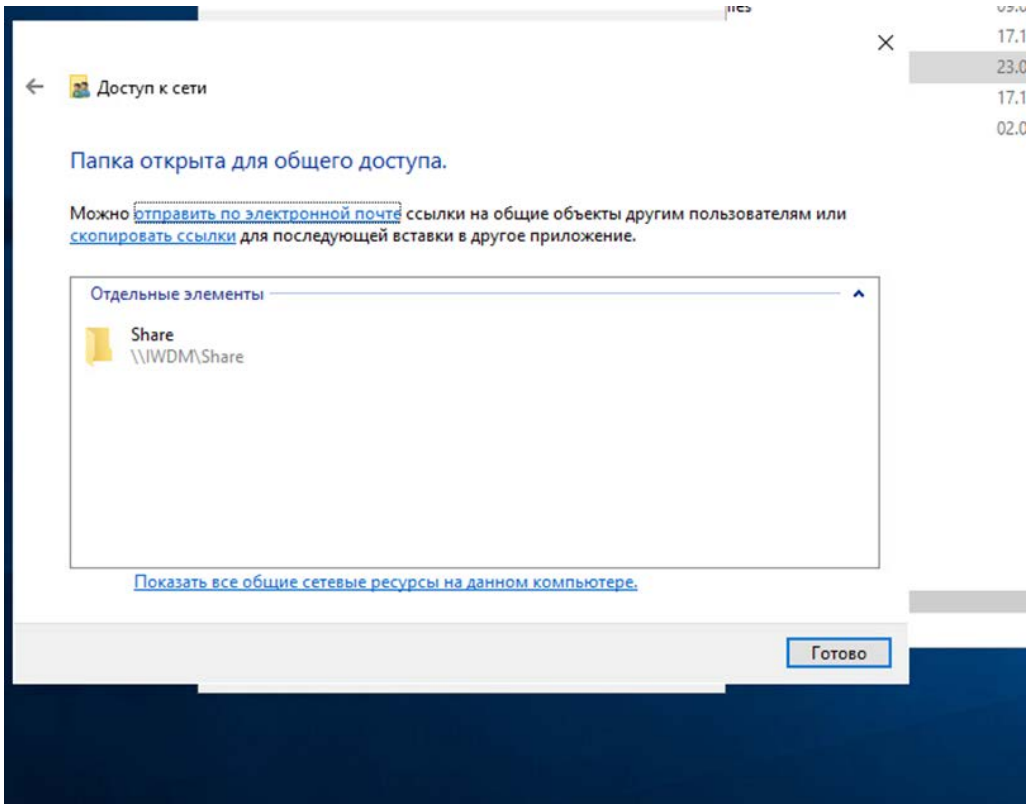


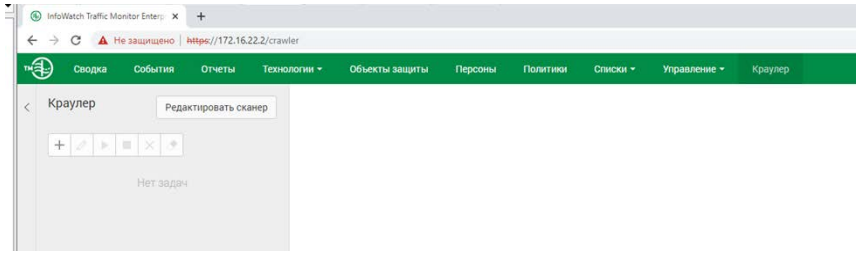
Изменить значение 0 на значение 1 напротив Crawler (спуститесь на одну строку ниже crawler и нажмите кнопку назад)



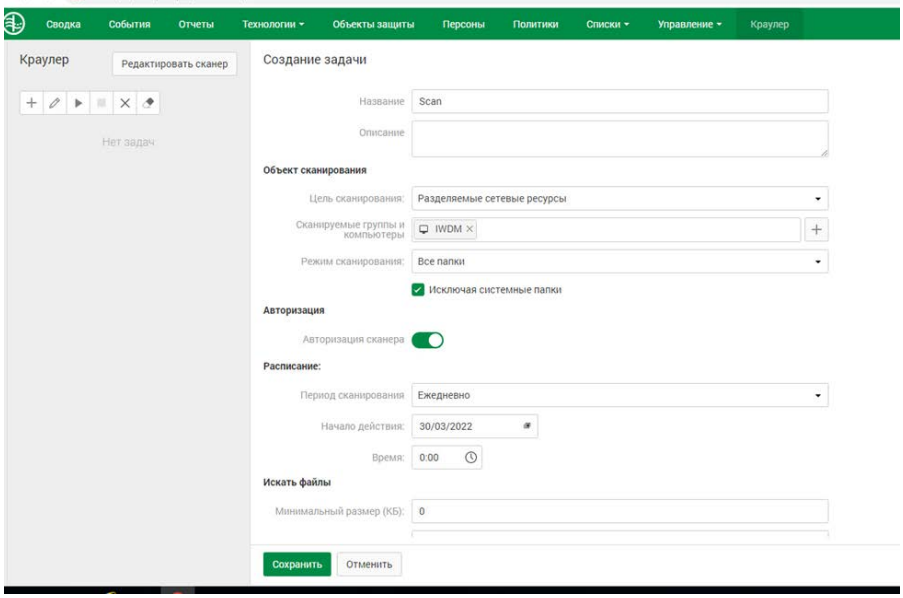

Выбор: "Пользователи" или "Группы"
Выберите тип объекта:
"Пользователи", "Группы" или "Встроенные субъекты безопасн
Типы объектов...
В следующем месте:
demo.lab
Размещение...
Введите имена выбираемых объектов (примеры):
Domain Users
Проверить имена
Дополнительно...
OK
Отмена
Проблемы при предоставлении общего доступа
Поделиться
Отмена

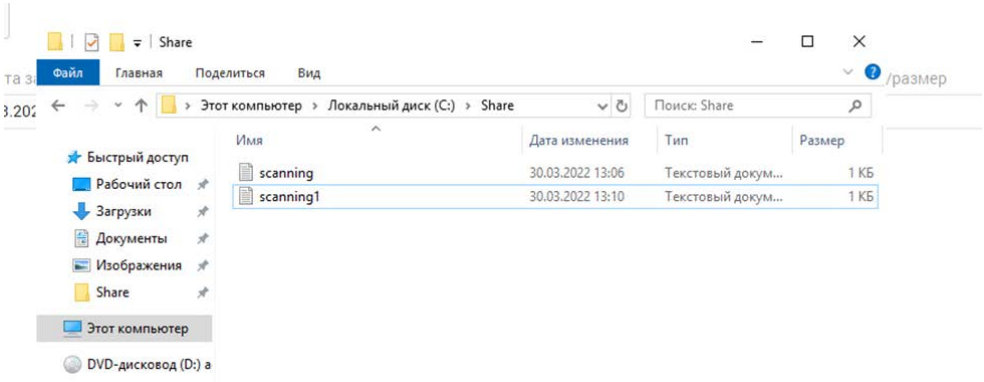

Доступ к сети
Выберите в сети пользователей, с которыми вы хотите поделиться
Введите имя и нажмите кнопку "Добавить" либо используйте стрелку для поиска определенного пользователя.
Добавить
Имя
Уровень разрешений
Domain Users
Чтение и запись
iw-admin
Владелец
Проблемы при предоставлении общего доступа
Поделиться
Отмена





Если же ваш краулер не отобразился, то проверьте выключен ли брэндмауэр на demo.lab и перезагрузите эту машину. Далее проверьте на iwtm наличие dns и также перезагрузите. IWDM лучше тоже перезапустить.





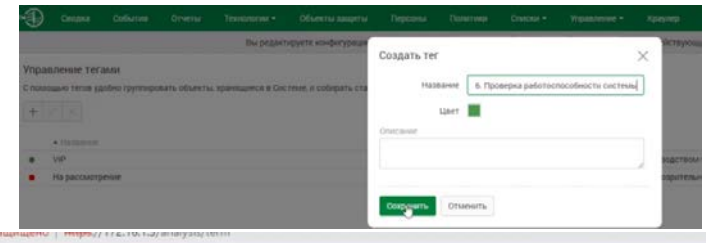
Сделать такой скрин!

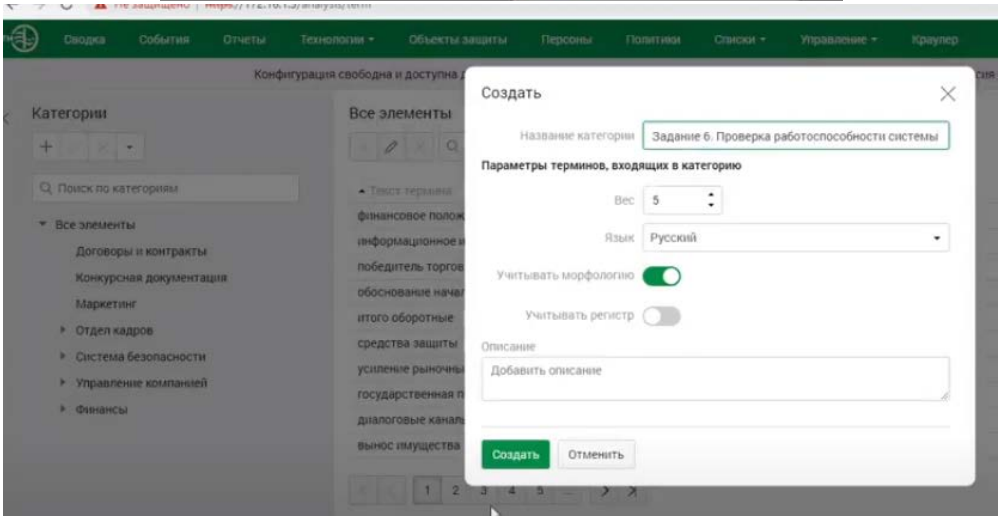
Задание 6: Проверка работоспособности системы

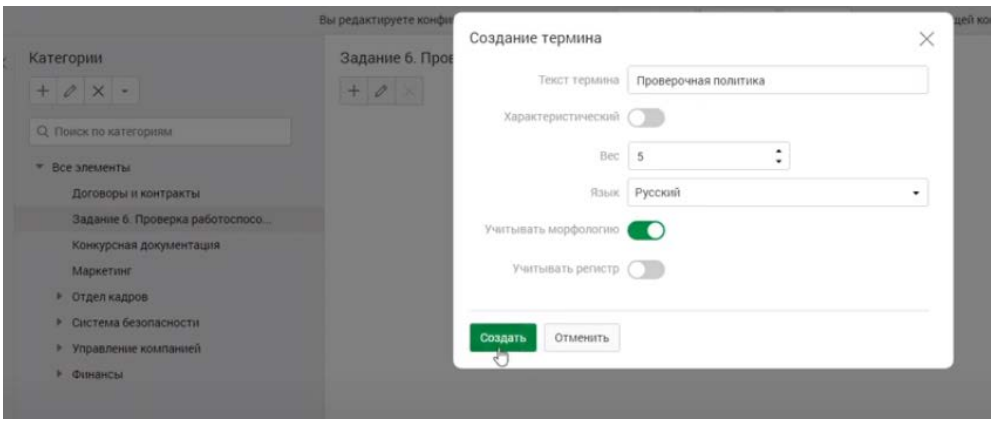
Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих некий термин, установить уровень угрозы для всех событий, добавить тег.

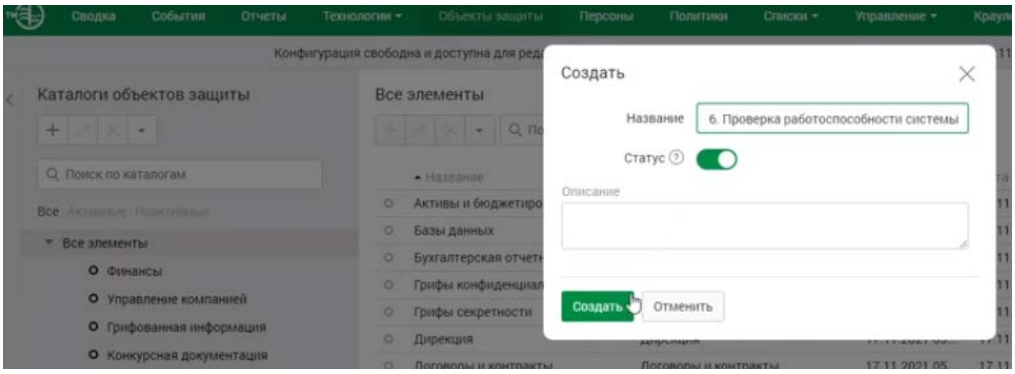
Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя 1 с установленным агентом. Сделать одну выборку, в которой будет отображено только по одному событию каждого типа, настроив конструктор выборки вручную.

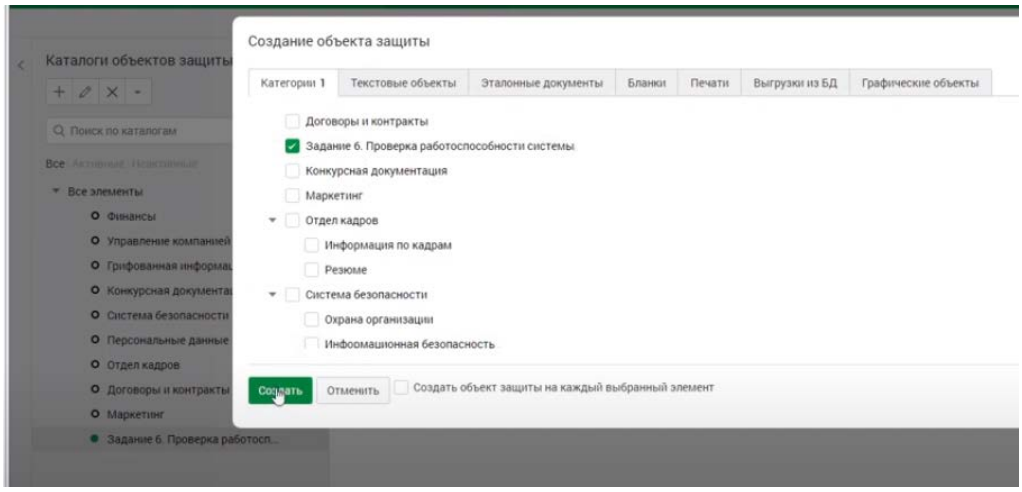
Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

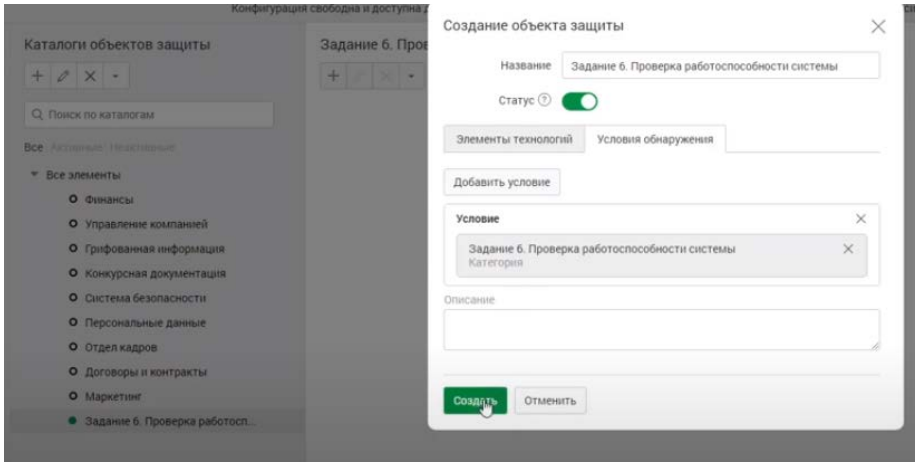


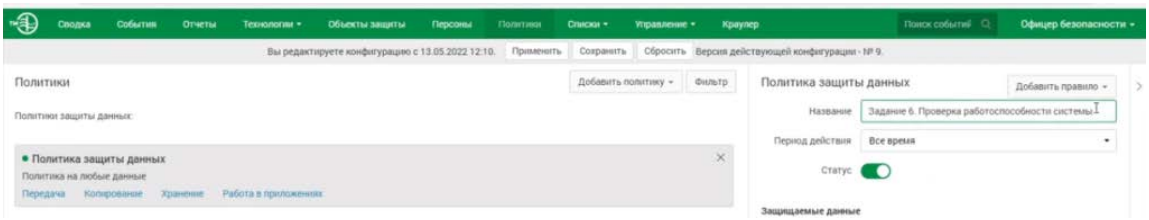


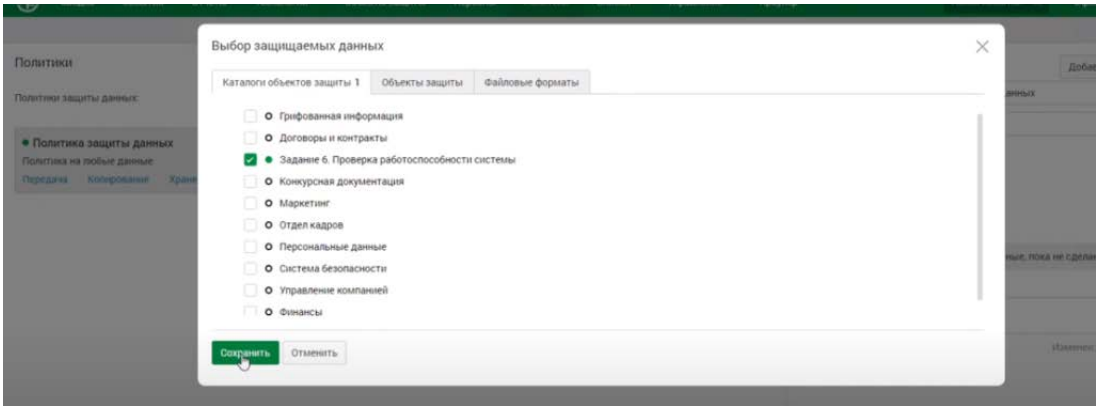

Категории
Поиск по категориям
Все элементы
Договоры и контракты
Задание 6. Проверка работоспосо...
Конкурсная документация
Маркетинг
Отдел кадров
Система безопасности
Управление компанией
Финансы
Создание термина
Текст термина
Проверочная политика
Характеристический
Вес
5
Язык
Русский
Учитывать морфологию
Учитывать регистр
Создать
Отменить

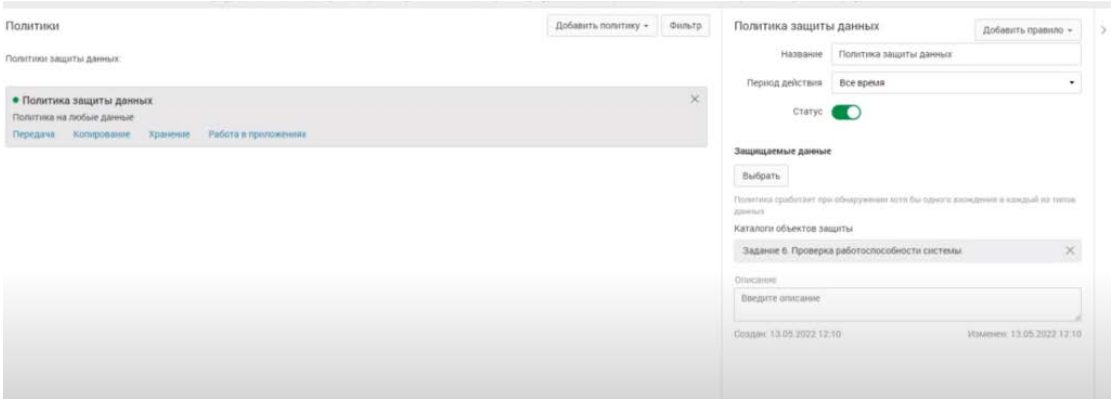

Сводка
События
Отчеты
Технологии
Объекты защиты
Персоны
Политики
Списки
Управление
Конфигурация свободна и доступна для ред
Каталоги объектов защиты
Поиск по каталогам
Все элементы
Финансы
Управление компанией
Грифованная информация
Конкурсная документация
Все элементы
Название
Активы и бюджетиро
Базы данных
Бухгалтерская отчет
Грифы конфиденциал
Грифы секретности
Дирекция
Создать
Название
6. Проверка работоспособности системы
Статус
Описание
Создать
Отменить

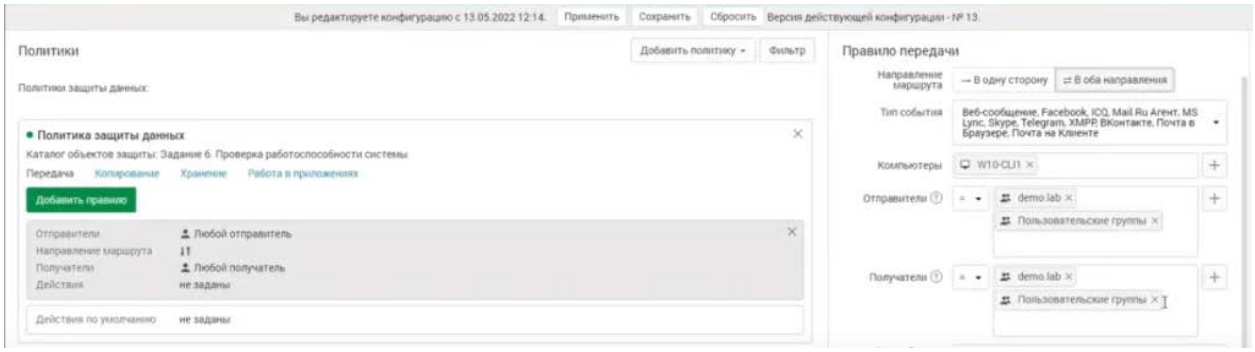

Каталоги объектов защиты
Поиск по каталогам
Все элементы
Финансы
Управление компанией
Грифованная информа
Конкурсная документа
Система безопасности
Персональные данные
Отдел кадров
Договоры и контракты
Маркетинг
Задание 6. Проверка работосп...
Создание объекта защиты
Категории 1
Текстовые объекты
Эталонные документы
Бланки
Печати
Выгрузки из БД
Графические объекты
Договоры и контракты
Задание 6. Проверка работоспособности системы
Конкурсная документация
Маркетинг
Отдел кадров
Информация по кадрам
Резюме
Система безопасности
Охрана организации
Инфоомационная безопасность
Создать
Отменить
Создать объект защиты на каждый выбранный элемент


Каталоги объектов защиты
Поиск по каталогам
Все элементы
Финансы
Управление компанией
Грифованная информация
Конкурсная документация
Система безопасности
Персональные данные
Отдел кадров
Договоры и контракты
Маркетинг
Задание 6. Проверка работосп...
Создание объекта защиты
Название
Задание 6. Проверка работоспособности системы
Статус
Элементы технологий
Условия обнаружения
Добавить условие
Условие
Задание 6. Проверка работоспособности системы
Категория
Описание
Создать
Отменить

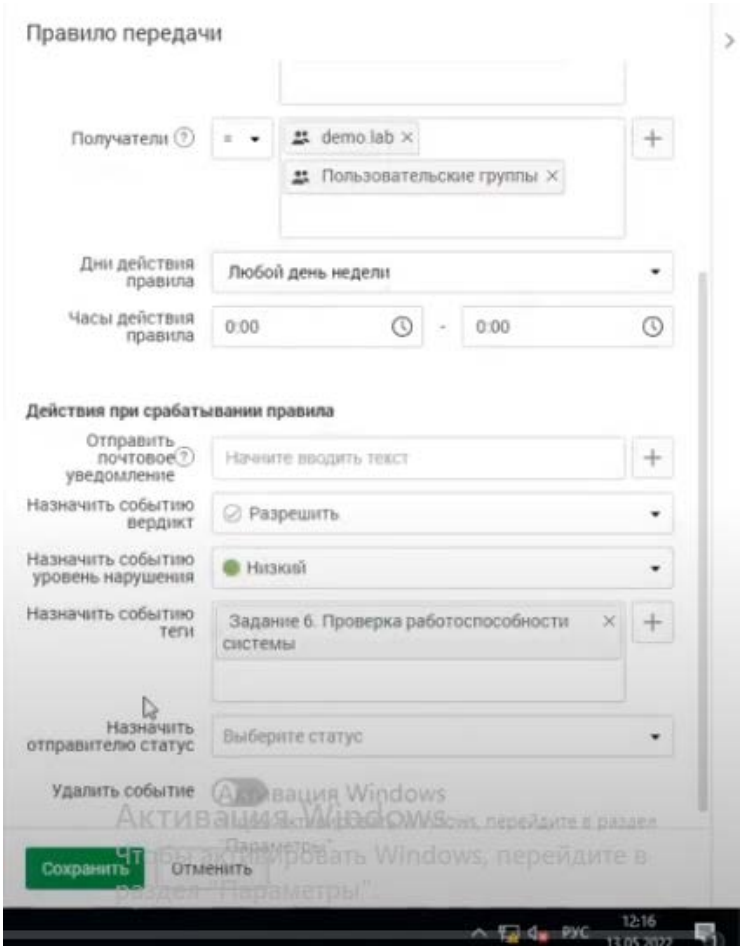


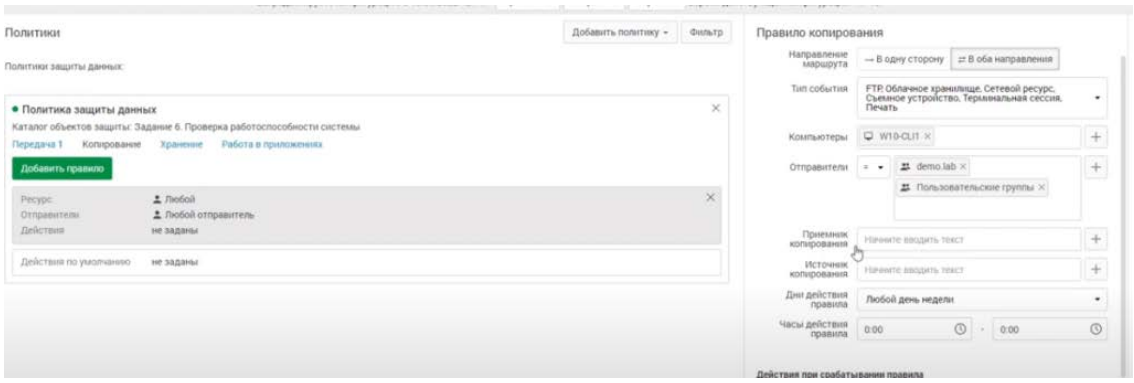




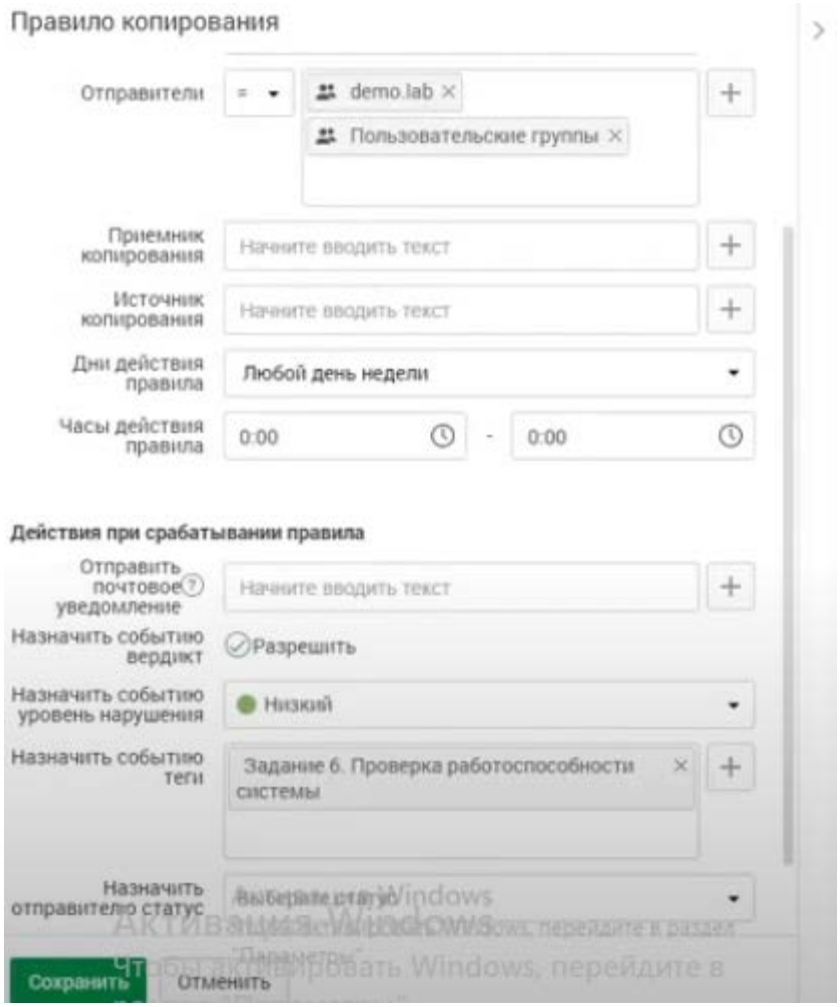


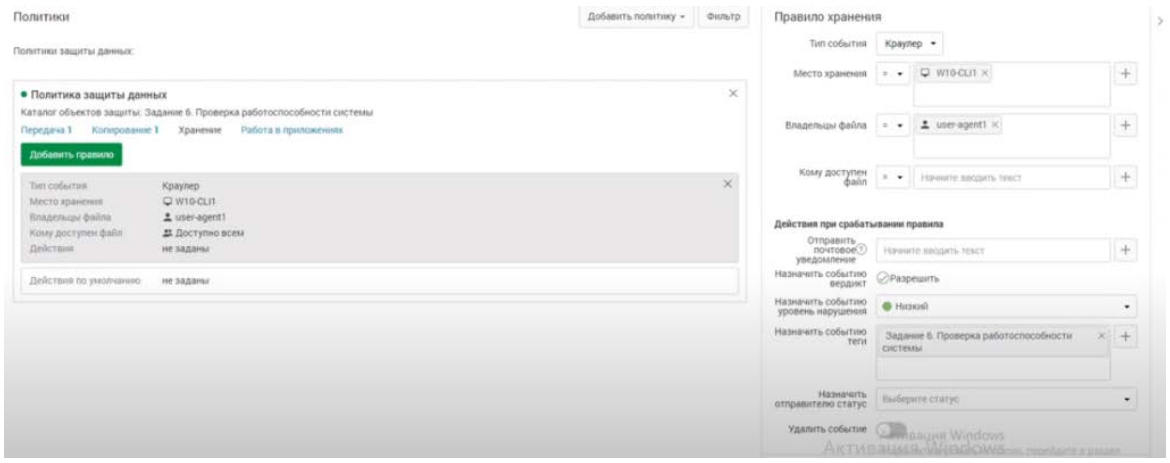
Делаем для передачи





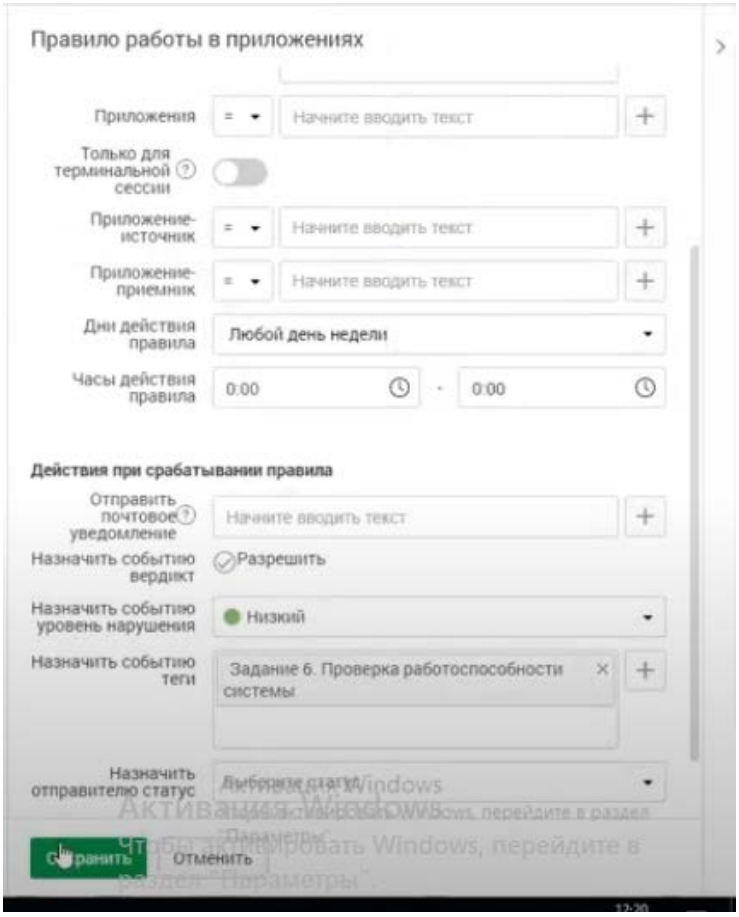
Для копирования


Правило копирования
Отправители
demo.lab
Пользовательские группы
Приемник копирования
Начните вводить текст
Источник копирования
Начните вводить текст
Дни действия правила
Любой день недели
Часы действия правила
0:00
0:00
Действия при срабатывании правила
Отправить почтовое уведомление
Начните вводить текст
Назначить событию вердикт
Разрешить
Назначить событию уровень нарушения
Низкий
Назначить событию теги
Задание 6. Проверка работоспособности системы
Назначить отправителю статус
Сохранить
Отменить


Политики
Добавить политику
Фильтр
Политики защиты данных:
Политика защиты данных
Каталог объектов защиты: Задание 6. Проверка работоспособности системы
Передача 1
Копирование 1
Хранение
Работа в приложениях
Добавить правило
Тип события
Краулер
Место хранения
W10-CLI1
Владельцы файла
user-agent1
Кому доступен файл
Доступно всем
Действия
не заданы
Действия по умолчанию
не заданы
Правило хранения
Тип события
Краулер
Место хранения
W10-CLI1
Владельцы файла
user-agent1
Кому доступен файл
Начните вводить текст
Действия при срабатывании правила
Отправить почтовое уведомление
Начните вводить текст
Назначить событию вердикт
Разрешить
Назначить событию уровень нарушения
Низкий
Назначить событию теги
Задание 6. Проверка работоспособности системы
Назначить отправителю статус
Выберите статус
Удалить событие

Хранение


Политики
Добавить политику
Фильтр
Политики защиты данных:
Политика защиты данных
Каталог объектов защиты: Задание 6. Проверка работоспособности системы
Передача 1
Копирование 1
Хранение 1
Работа в приложениях
Добавить правило
Тип события
Буфер обмена
Компьютер
W10-CLI1
Приложение-источник
Любое приложение
Приложение-приемник
Любое приложение
Действия
не заданы
Действия по умолчанию
не заданы
Правило работы в приложениях
Тип события
Буфер обмена
Ввод с клавиатуры
Персоны
user-agent1
Компьютеры
W10-CLI1
Приложения
Только для терминальной сессии
Приложение-источник
Начните вводить текст
Приложение-приемник
Начните вводить текст
Дни действия правила
Любой день недели
Часы действия правила
0:00
0:00



Сделать конечный скрин политики

Задание 7: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям, параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги). Дерево сертификатов должно включать:

1. корневой root-сертификат (ca)
2. серверный (server) сертификат
3. по желанию допускается использование пользовательского и промежуточного сертификата.

Атрибуты для сертификатов:

Страна: RU
Область: Tomskaya
Организация: WorldSkills
Город: Tomsk
Отдел организации: IT
E-mail: support@demo.lab

После генерации сертификатов необходимо установить серверный сертификат на веб-сервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети для доверенного подключения к веб-консоли DLP-системы уровня сети. Итоговый результат должен включать:

Дерево из 2-3 сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе. Содержимое команд по генерации ключей и сертификатов в текстовом файле на рабочем столе с комментариями. Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).

Описание модуля 2:

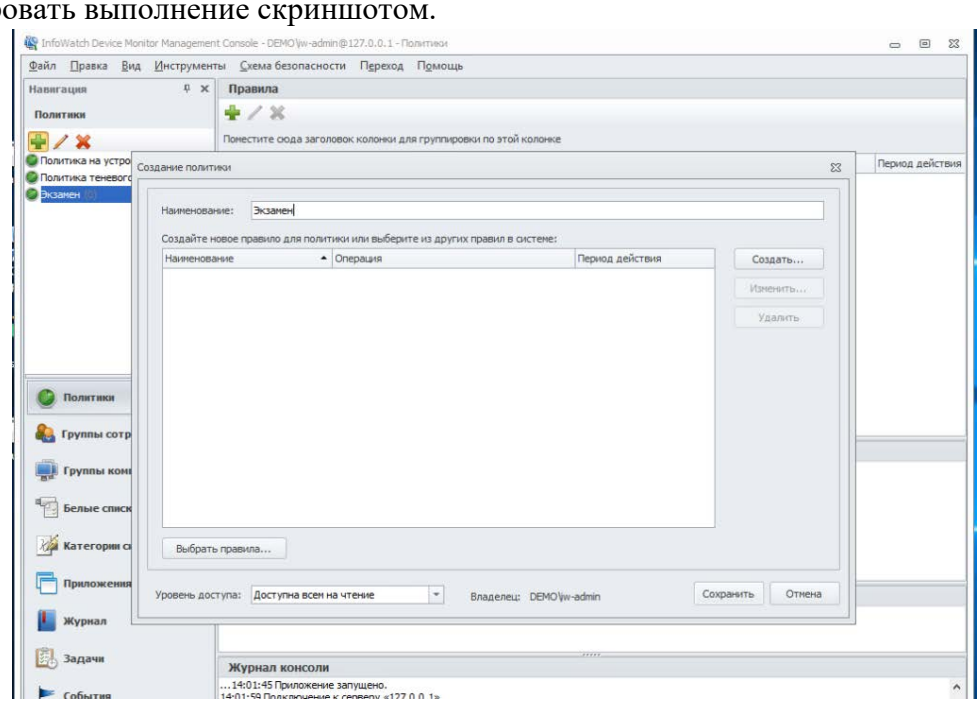
Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании). Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например, «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна. Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно).

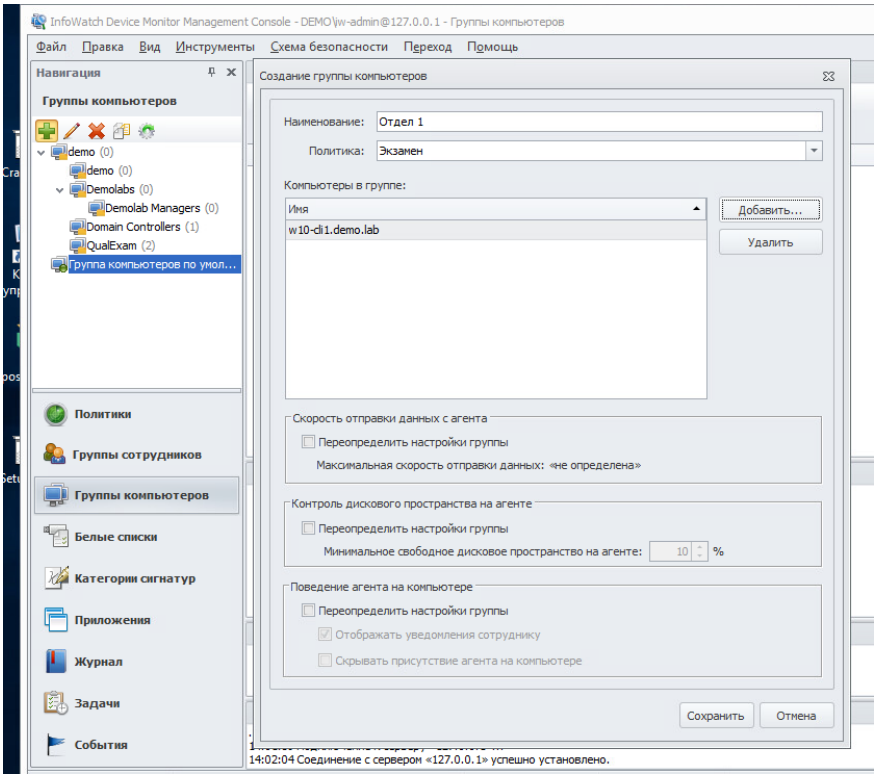
Задание 1

Необходимо создать 2 новых группы компьютеров: «Отдел1» и «Отдел2», а также создать 2 новых политики: «Отдел1» и «Отдел2». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 необходимо перенести в Отдел1, а компьютер 2 — в Отдел2.

Зафиксировать выполнение скриншотом.



Переходим во вкладку «группы компьюеров»



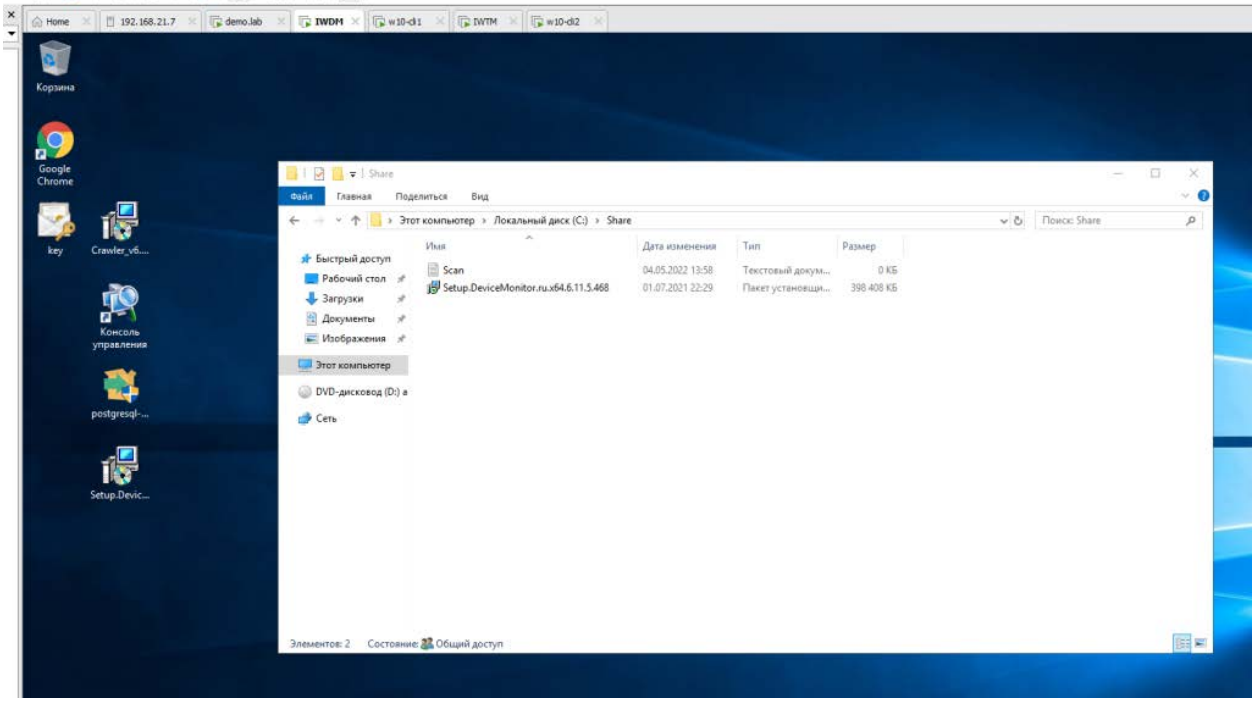
Сделать такой скрин!

По аналогии сделать вторую политику

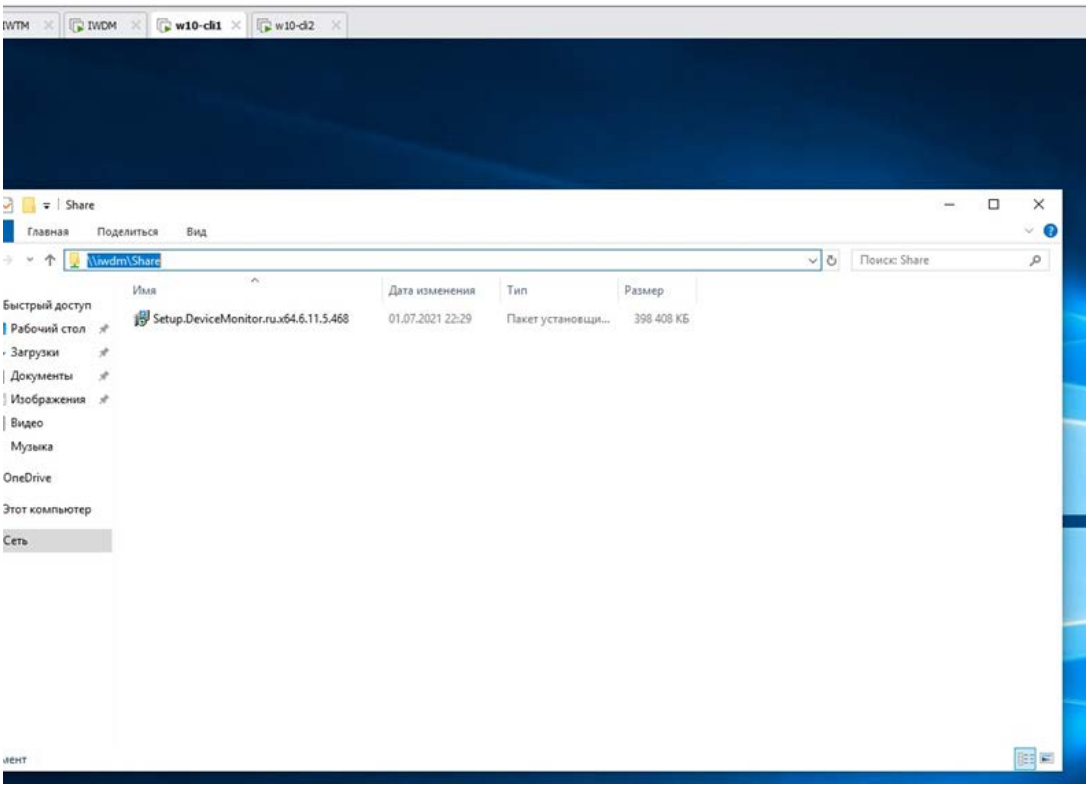
Задание 2

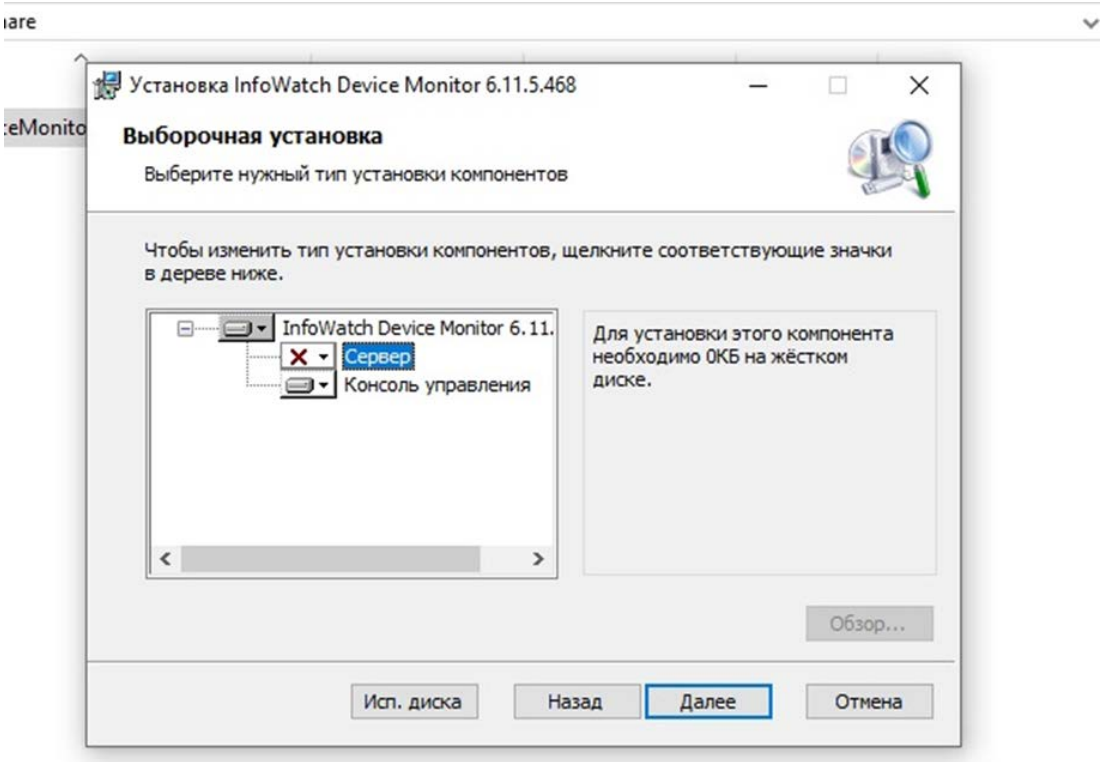
Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину W10-agent1 для удаленного доступа к серверу агентского мониторинга.

Следующие правила создаются в политике «Отдел1».



Не копируем, а полностью переносим





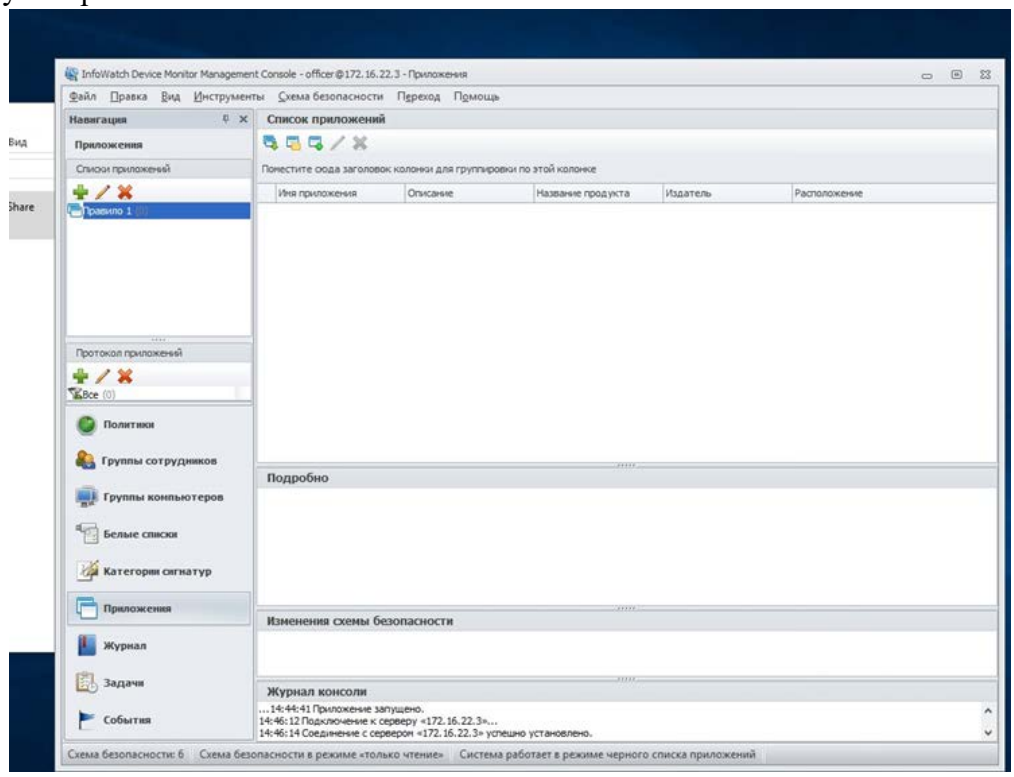
в консоль управления использовать ip iwdm
Следующие правила создаются в политике «Отдел1».
Правило 1

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

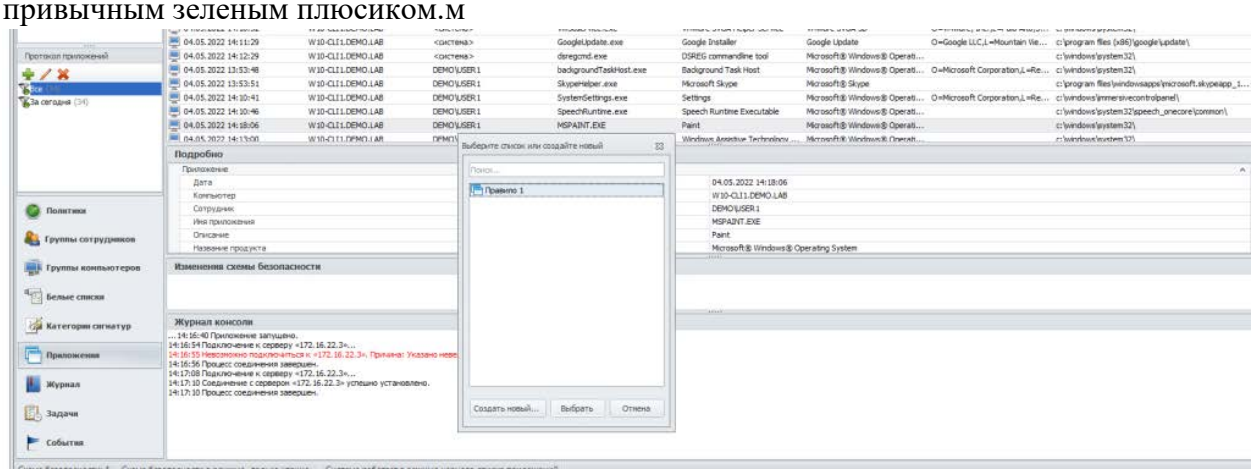
Проверить работоспособность и зафиксировать выполнение скриншотом.

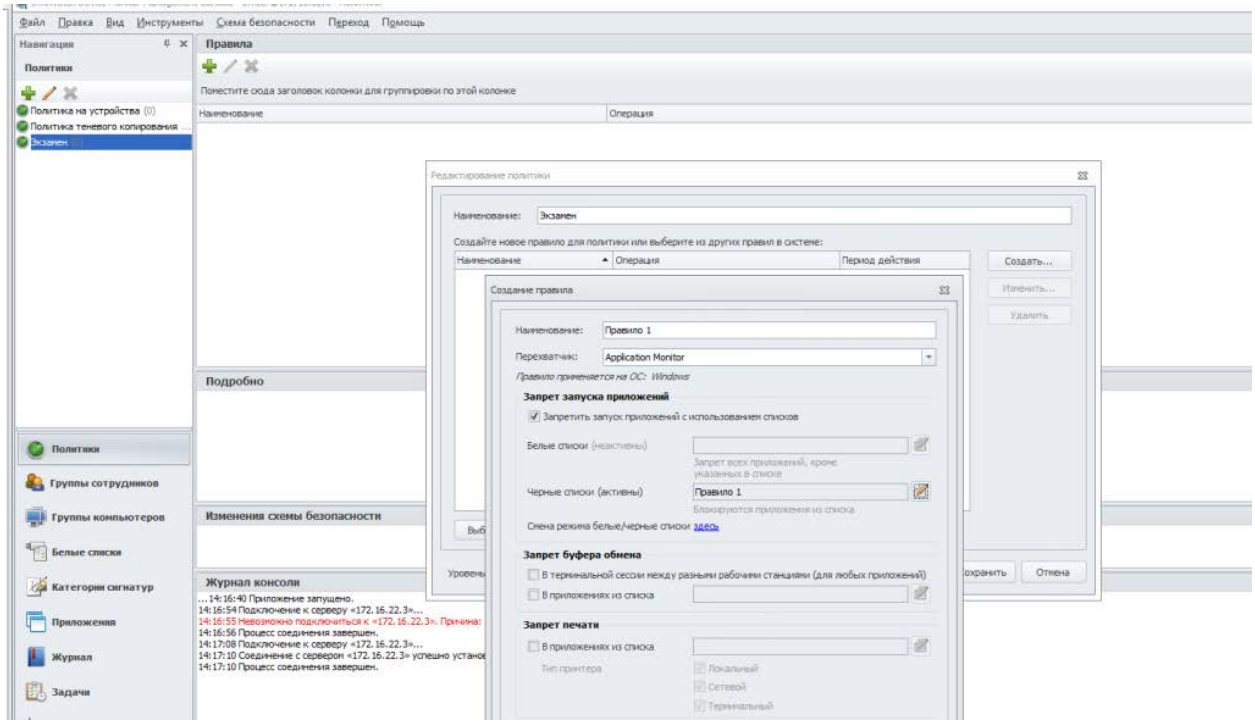
Ответ: Создание списков приложений. На каждое правило отдельный список желательно.

Лучше работать в консоли на клиенте.

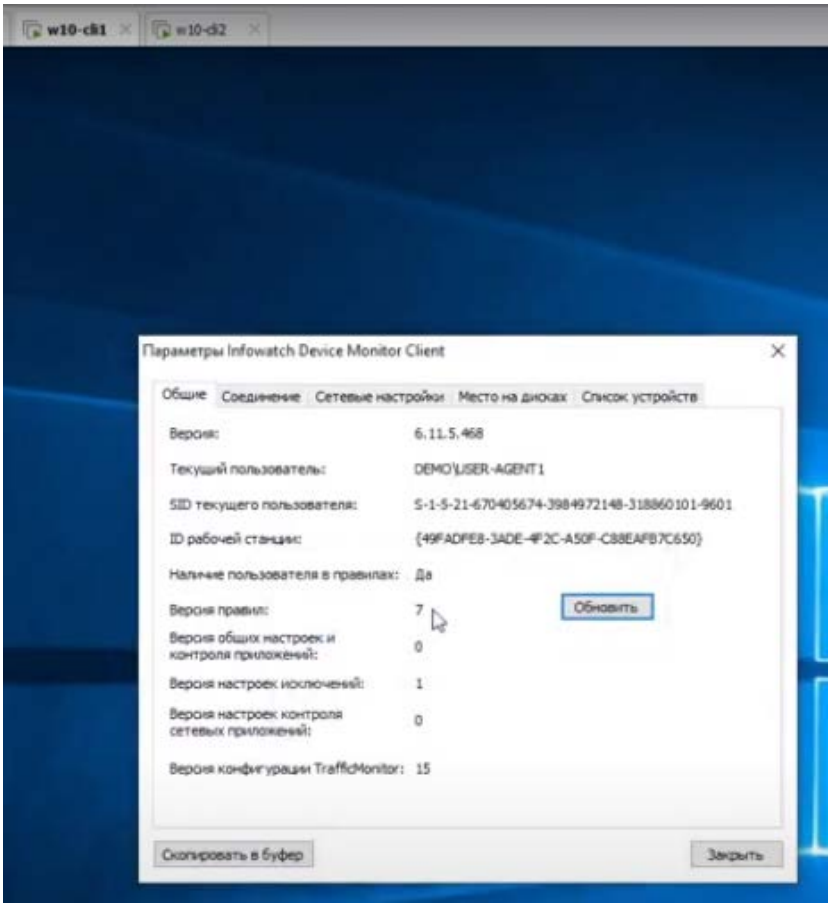


Для того, чтобы создать и настроить правило, вам необходимо вернуться к разделу «Политики» в Device Monitor Console и перейти к политики «Экзамен», после чего нажать кнопку «Создать правило…» (не путать с «создать политику…») обозначенную уже привычным зеленым плюсиком.м





Сделать такой скрин



Проверка правила — обновить и попробовать запустить paint, после каждого правила обновлять Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Перед этим также как и при создании первого правила требуется создать список (во вкладке приложения) и внести в него calc (excel отсутствует) — перед этим нужно запустить это приложения найдя его в поисковике windows

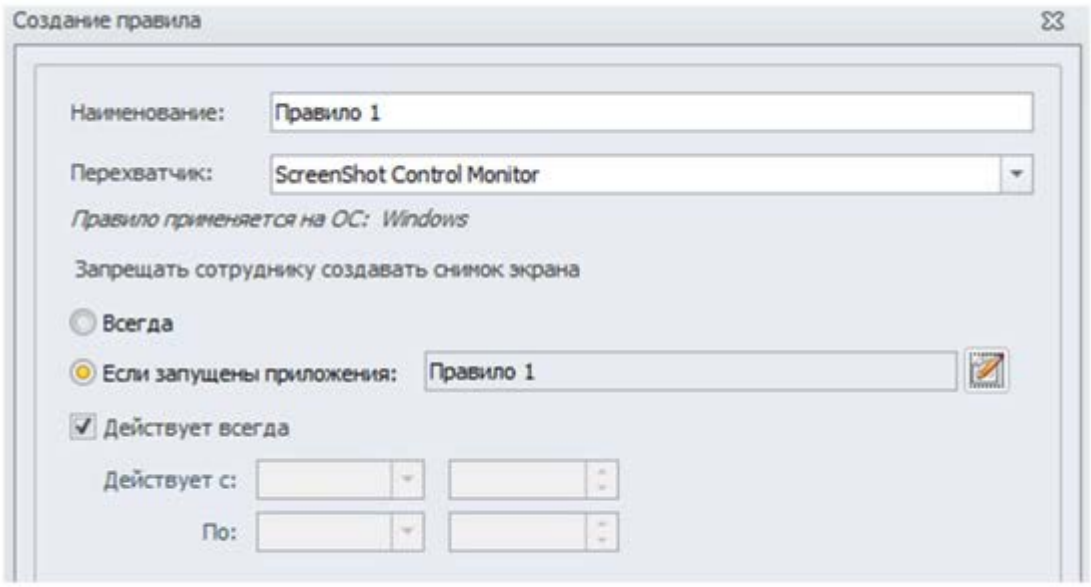
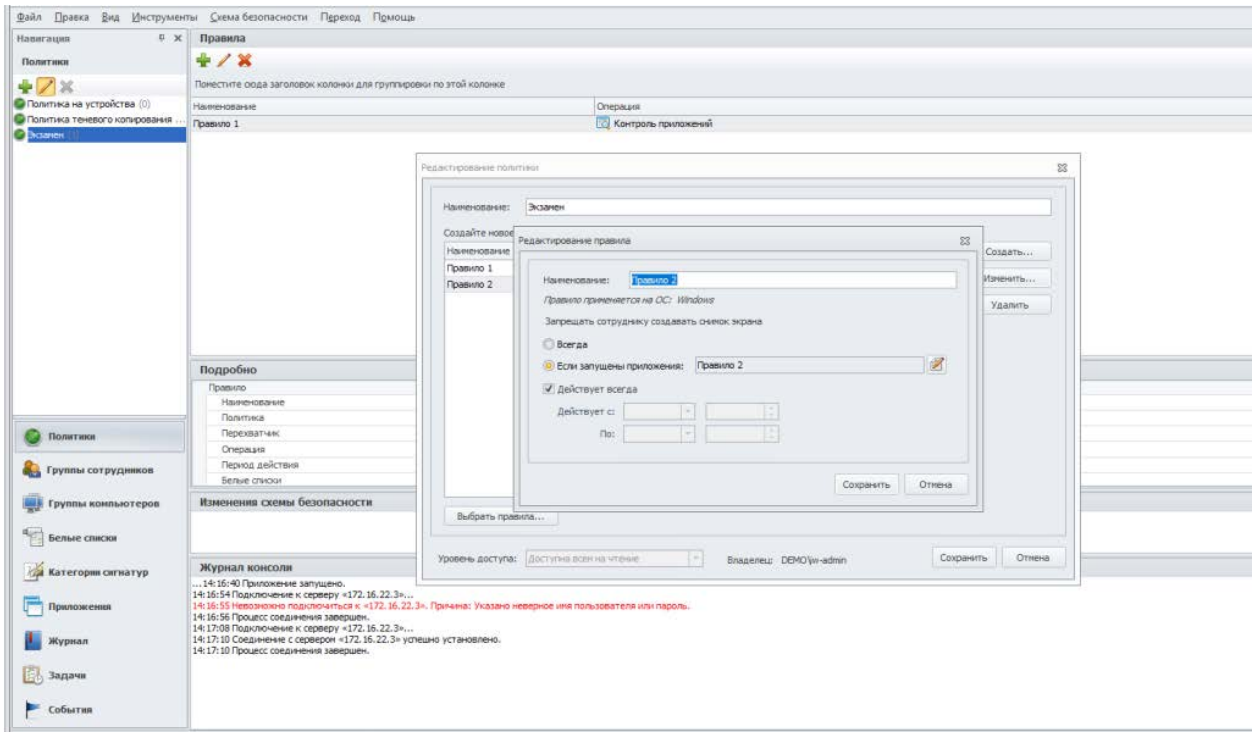
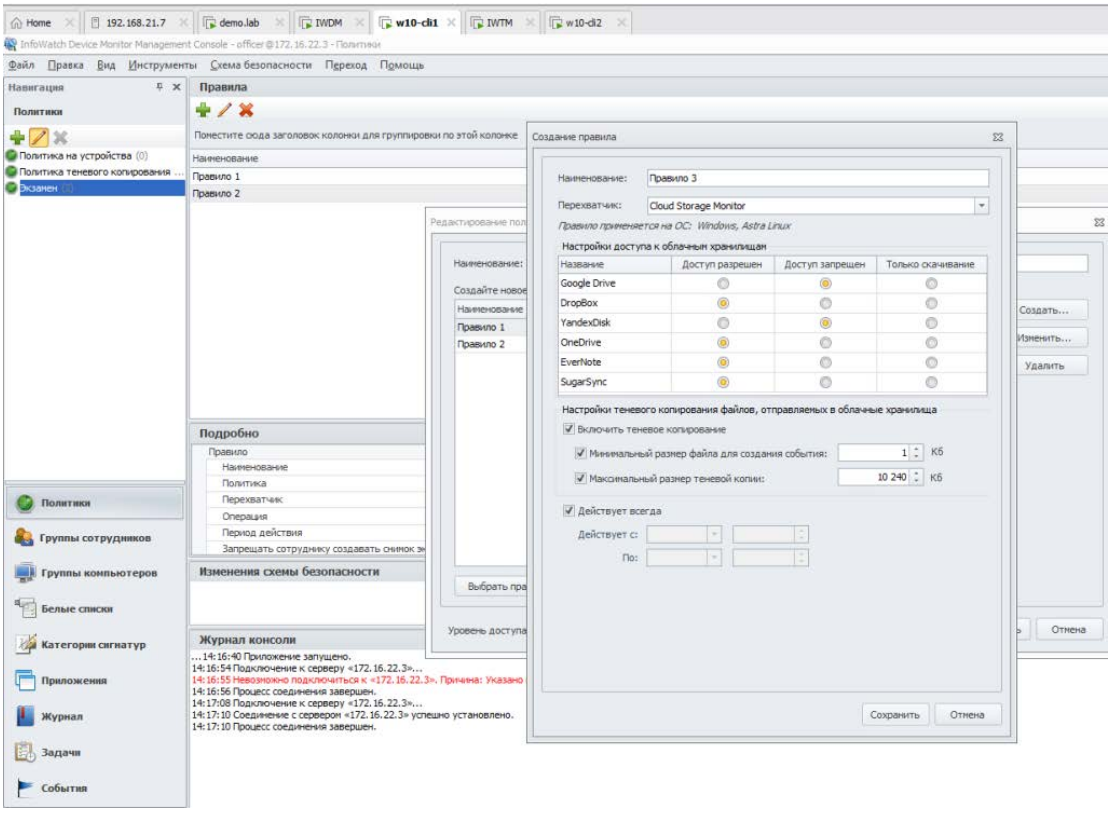


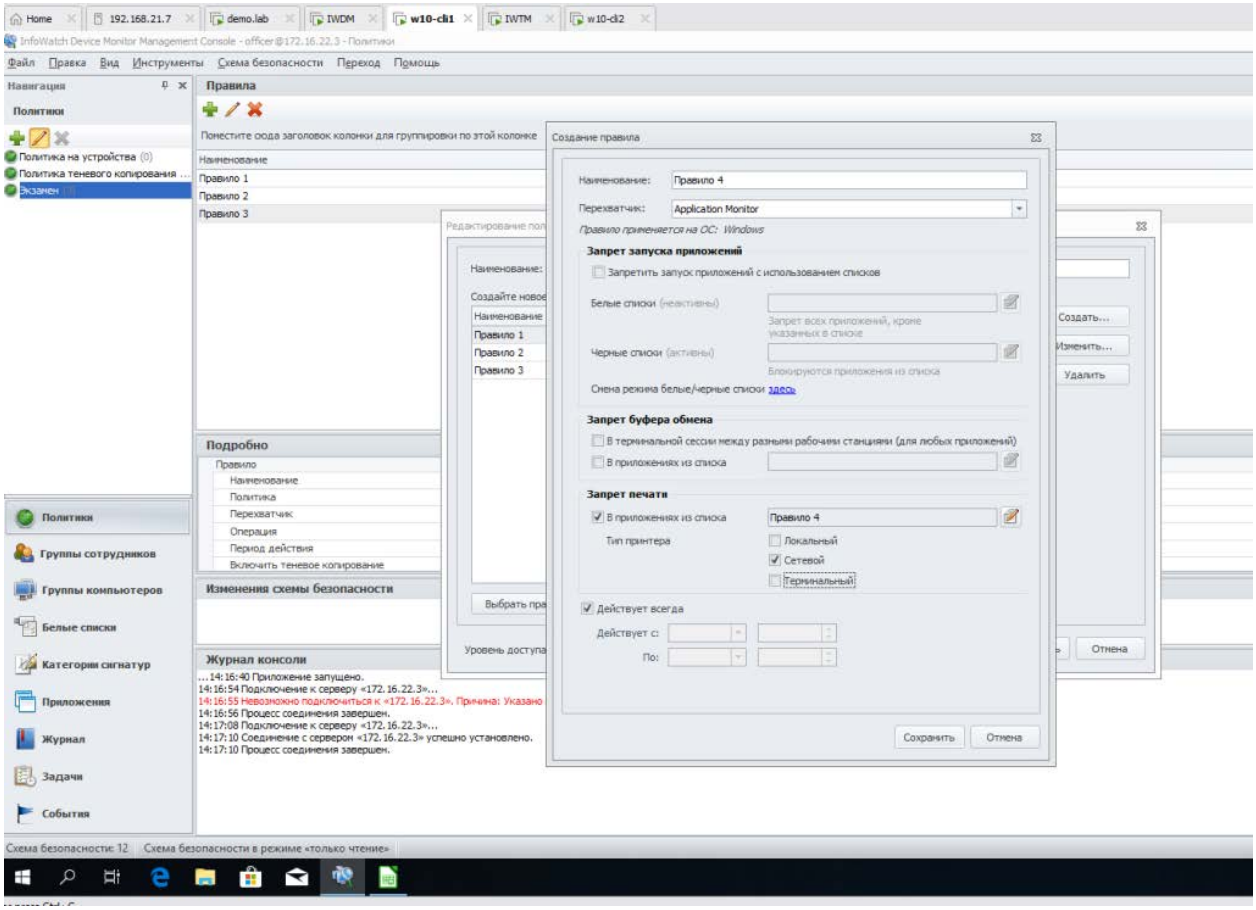
Рисунок 60 – «Правило 1»



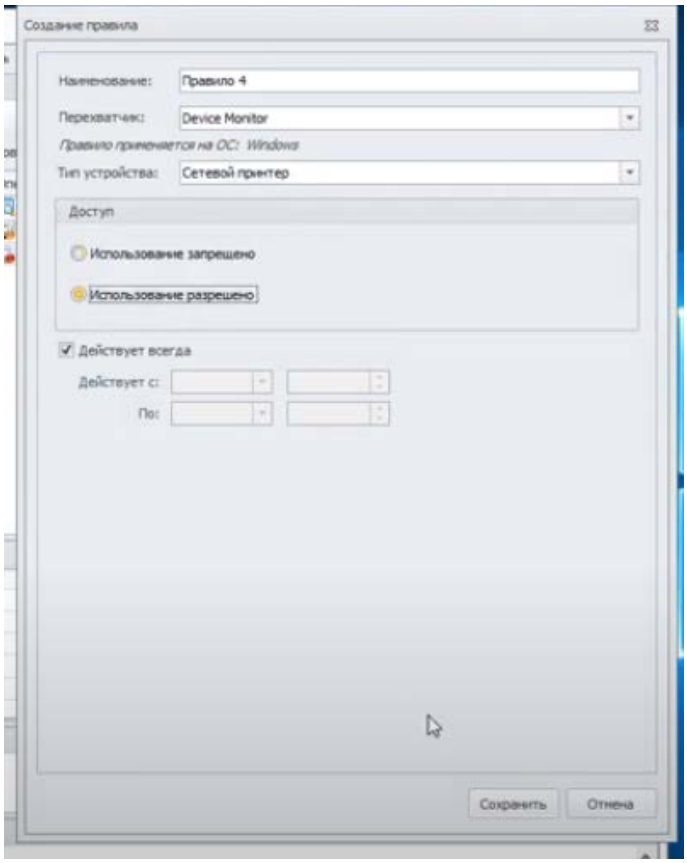
Сделать такой скрин
Правило 3
Ограничить доступ к облачным хранилищам GoogleDrive и YandexDisk.
Проверить работоспособность и зафиксировать выполнение



Здесь не создаем список, а сразу переходим в политику. Сделать такой скрин
Правило 4
Необходимо запретить печать на сетевых принтерах.
Зафиксировать создание политики скриншотом.
Создаем список и добавляем в него все приложения есть



Сделать такой скрин



Задание 4

Необходимо создать виджет в разделе сводка во вкладке «Дополнительные сводки» отображающий события с высоким уровнем угрозы на правила копирования за последние 7 дней.

Зафиксировать скриншотом конструктора выборки.

Задание 5

Необходимо создать виджет в разделе «Сводка», вкладка «Дополнительные сводки» для отображения нарушений только от обоих компьютеров нарушителей (виртуальных машин) со средним и высоким уровнем угрозы за последние 3 дня.

Зафиксировать скриншотом конструктор выборки.

Практическое занятие № 23-27

Тема: Разработка и применение политики агентского мониторинга для работы с файлами.

Цель: разработать и применить политику агентского мониторинга для работы с файлами.

Теоретическая часть:

Применение агента Zabbix

Ранее мы устанавливали своего агента Zabbix на том же самом хосте и выполняли мониторинг для него единственный элемент. Настало время расшириться и посмотреть как работает связь между хостами.

Для продолжения установите агента Zabbix на другом хосте. Самый простой способ может быть установкой из пакетов распространения - либо вы можете выбрать его компиляцию из исходного кода. Если вы устанавливаете из пакетов в системах на основе систем Red Hat Enterprise Linux (RHEL)/ Debian, обратитесь к Главе 1, Приступая к работе с Zabbix. Потенциально названием пакета агента может являться zabbix-agent.

Компиляция такого агента только из исходного кода делается аналогично тому как все компоненты включались для компиляции в Главе 1, Приступая к работе с Zabbix. Вместо полной строки configure мы будем применять на этот раз единственный флаг:

```
$ ./configure --enable-agent
```

Настройка должна завершиться успешно и важны такие итоговые строки:

```
Enable server:         no
Enable proxy:          no
Enable agent:          yes
```

Если полученный вами вывод соответствует только что приведённому, продолжите вызовом такой команды:

```
$ make install
```

Компиляция должна завершиться без каких бы то ни было ошибок и должна быть выполнена относительно быстро. Однако мы должны быть в курсе, что скомпилировали своего агента без поддержки для шифрования. В конце данной главы я добавил URL для документации, которая поясняет какие параметры требуются для добавления шифрования.

Если вы устанавливаете пакеты распространения в некотором дистрибутиве, отличающемся от того где установлен сервер, не беспокойтесь в том случае когда получаемый демон агента имеет более старую версию чем сам сервер. Такой вариант поддерживается и должен работать как положено. Тем не менее, если ваш агент старше чем 1.4, он не будет работать в Zabbix 4.0, так как были произведены изменения в том как сам агент взаимодействует со своим сервером Zabbix. Более новый агент со старым сервером может не работать и эта ситуация не поддерживается. Вам следует избегать применение некого раннего сервера с более новыми агентами, если только это не было проверено с тем чтобы гарантировать что такая комбинация будет работать как положено.

Сохранение более старого агента может быть более удобным если вы уже имеете его установленным и его работа устраивает вас. При установке более нового предполагается, что вы будете работать с самым последним, так как он может иметь исправленными найденный ошибки, лучшую производительность, большее число поддерживаемых элементов для определённой платформы и прочие преимущества.

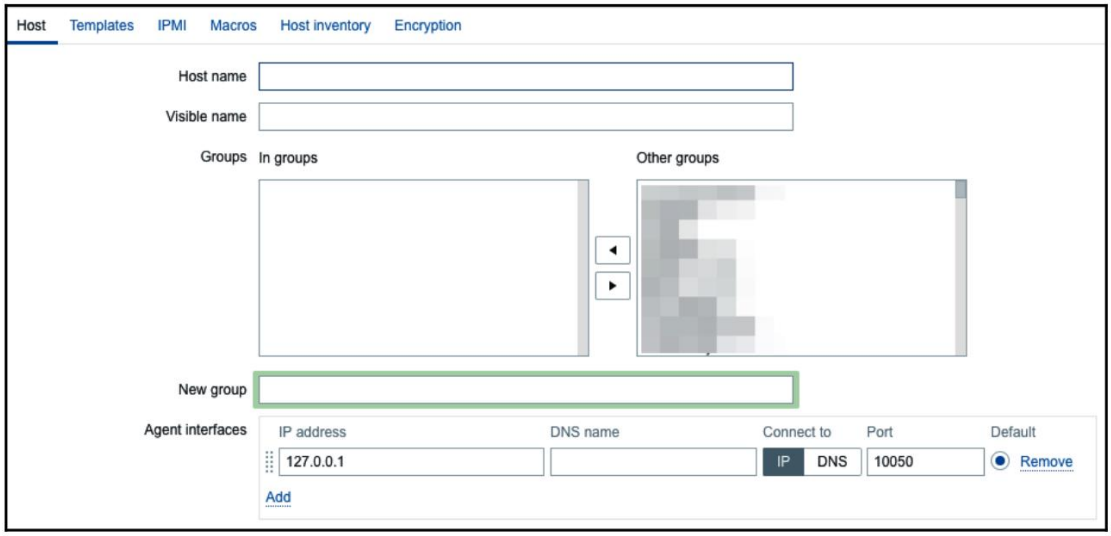
После установки соответствующего агента самое время запустить его. Как это сделать целиком определяется вашим методом установки - и если вы выполняли установку из соответствующих пакетов, это также зависит и от самого дистрибутива. За примерами того как запускать вашего агента отсылаем к Главе 1, Приступая к работе с Zabbix. В качестве быстрого напоминания, если вы устанавливали из пакетов в системе на основе RHEL/Debian, ваш агент вероятно можно запустить как- то так:

```
# systemctl start zabbix-agentd
```

Если вы устанавливали из исходного кода, напрямую исполните свой исполняемый файл:

```
# <path>/zabbix_agentd
```

После того как этот агент запущен, нам также придётся добавить этот новый хост в свои настройки:



Вот несколько советов по заполнению данной формы:

Host name: Не сдерживайте себя в том чтобы присвоить содержательное нащвание, либо просто введите Another host

Agent interfaces: Заполните либо IP address, либо DNS name в зависимости от применяемого вами метода подключения

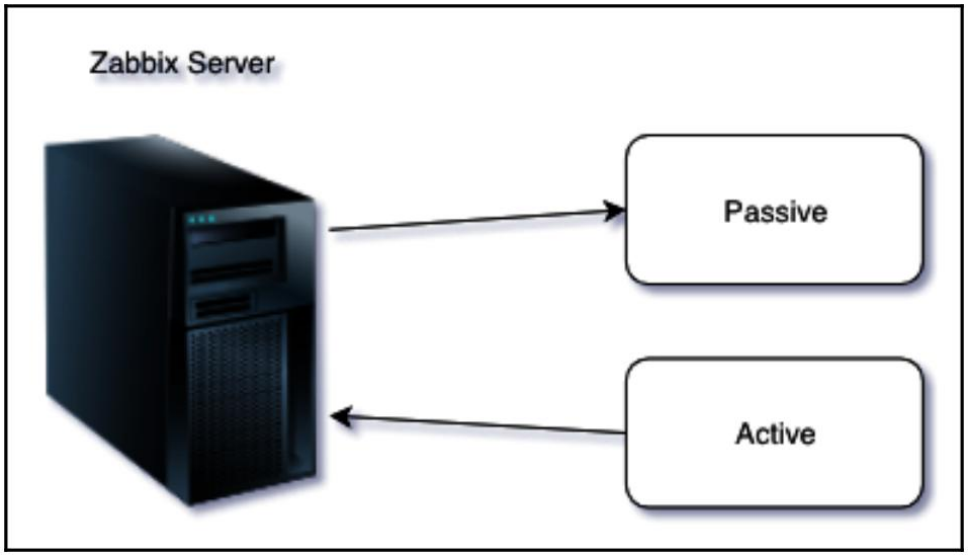
Connect to: Если вы решили следовать с DNS name, переключите в DNS

По завершению кликните по кнопке Add в самом низу.

Пассивные элементы

Тот элемент, который мы создали ранее был так называемым пассивным элементом, что означает что сам сервер Zabbix инициирует некое подключение к такому агенту всякий раз, когда осуществляется сбор его значения. В большинстве случаев они просто именуются как являющиеся типом агента Zabbix.

Чтобы проще запомнить пассивный или активный в Zabbix лучше рассуждать с точки зрения самого агента. Если к серверу подключается сам агент, он является активным. Если это не так - он пассивный:



Давайте создадим другой пассивный элемент для проверки своего удалённого хоста:

Перейдите в Configuration | Hosts.

Кликните по Items вслед за тем хостом, который вы только что создали.

Кликните по кнопке Create item. Это создаст наш пассивный элемент, поэтому убедитесь что он в точности такой, как мы его описываем здесь. В данном элементе мы попытаемся отслеживать состояние своего веб сервера когда он уже запущен в качестве нашего интерфейса с портом 80:

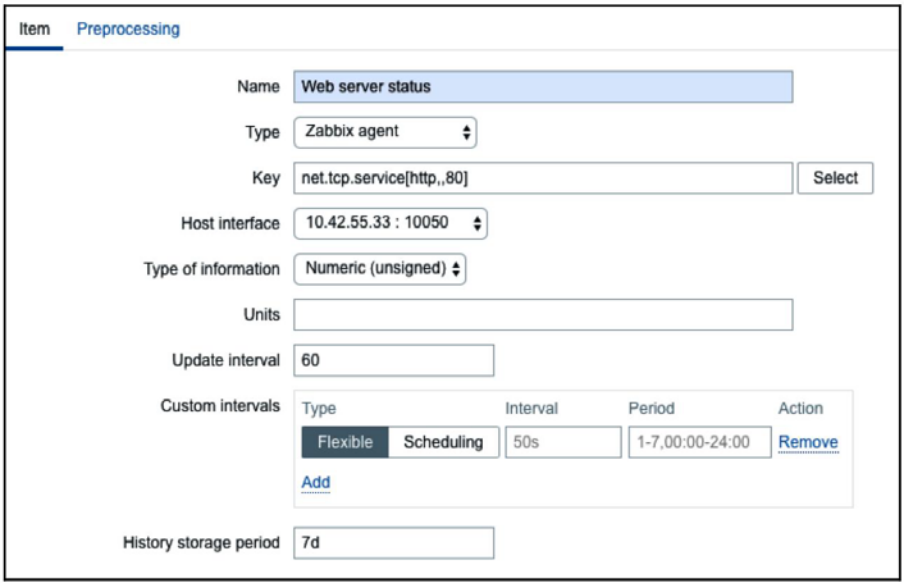
Name: Введите Web server status

Key: Введите net.tcp.service[http,,80] (перед 80 имеются две последовательные запятые)

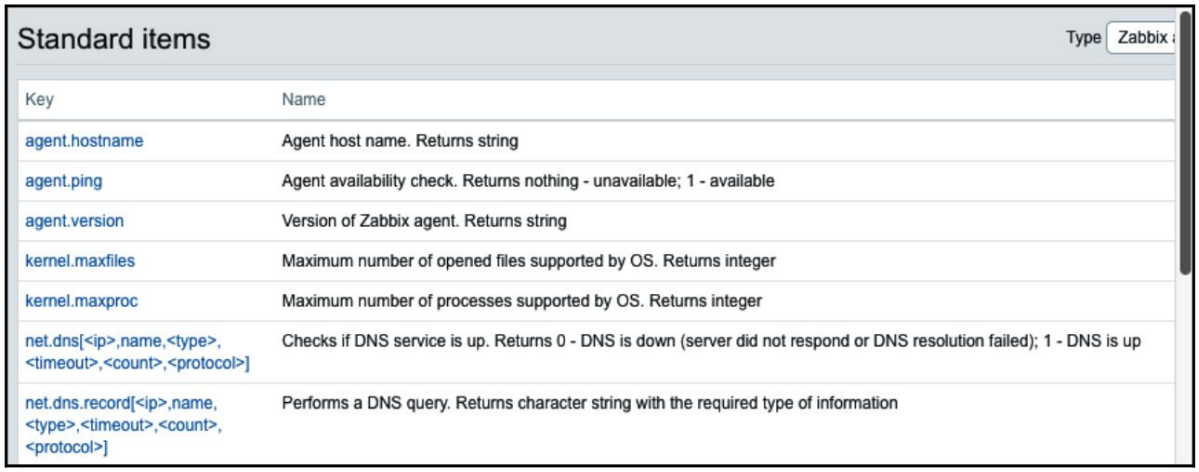
Update interval: Измените на 60 с установленного по умолчанию значения (30) - поскольку минуты должно быть более чем достаточно для наших целей

History storage period: Измените на 7 с установки по умолчанию (90) - это всё же сохранение целой недели с в точности поминутным обслуживанием

Наш окончательный результат должен выглядеть похожим на следующий снимок экрана:



Но что произошло с тем самым „80 добавленным к названию этой службы? Кликните по кнопке Select следующей за полем Key. Это откроет некое окно с отличным списком ключей для выбора из него совместно с кратким описанием каждого из них:



Ниспадающее меню Type в правом верхнем углу позволит вам переключаться между некоторыми типами элементов - мы обсудим все прочие типы позднее. А сейчас отыщите в этом списке net.tcp.service и просмотрите его описание. Здесь следует изучить два момента:

Прежде всего, на самом деле нам нет нужды добавлять это значение 80 - то есть порт, а принимая во внимание что значением по умолчанию уже является 80, его добавление является избыточным. Тем не менее, будет полезно если у вас будет некая служба, запускаемая с каким- то нестандартным портом.

Во- вторых, существует перечень ключей всего в один клик чтобы предоставить вам быструю подсказку в том случае если вы позабыли конкретный ключ или какими должны быть параметры.

Данный ключ, net.tcp.service слегка особенный: он пытается проверить что соответствующая служба отвечает стандартным манером, что означает, что такая служба явно должна поддерживаться. На момент написания Zabbix поддерживал такие службы для ключа net.tcp.service:

FTP
HTTP
HTTPS
IMAP

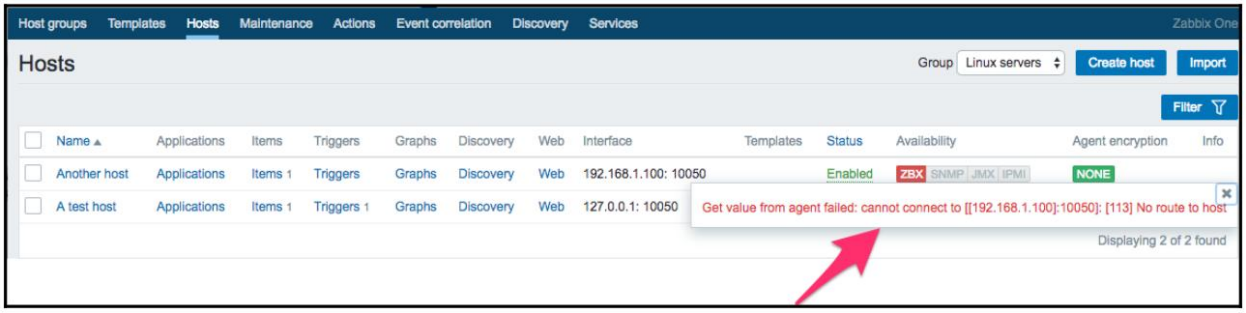
LDAP
NNTP
POP
SMTP
SSH
TCP
Telnet
NTP

Служба TCP является слегка особенной своим собственным образом. В то время как все прочие осуществляют соответствующие службе проверки, TCP в действительности не является службой; это просто проверка наличия подключения TCP. Он ближе к некому ключу, который мы рассматривали парой строк выше в своём списке элементов, net.tcp.service. Как пишет его описание, этот пункт пытается открыть некое подключение TCP по любому произвольному порту без выполнения каких- либо относящихся к службе проверок относительно возвращаемого значения. Если вы попытаетесь применить некую произвольную строку, которая не поддерживается, вы просто получите сообщение об ошибке, которое проинформирует, что такой ключ элемента не поддерживается.

Не сдерживайте себя и просмотрите прочие доступные ключи - мы также будем применять пару из них позднее - затем закройте это всплывающее меню и кликните по кнопке Add в самом низу. Вы вероятно уже заметили зелёную полоску в самом верху своего экрана после успешного завершения некоторой операции. В более ранних версиях было доступным некое управление с названием Details. Начиная с Zabbix 4.0 это было изменено и теперь мы более не наблюдаем никаких подробностей, только то что данный элемент был добавлен:

Теперь мы можем проследовать в Monitoring | Latest data и дождаться здесь появления необходимых значений, но это было бы никуда не годным. Вместо этого после пары минут вам следует посетить Configuration | Hosts. В зависимости от настроек вашей сетевой среды, вы можете увидеть некий красный маркер ZBX вслед за этим хостом. Эта иконка представляет ошибки, которые произошли при попытке выборки данных с некоторого пассивного агента Zabbix.

Чтобы посмотреть реальные сообщения об ошибках, переместите курсор мыши на эту иконку и вам откроется контекстное меню. Кликните по соответствующей иконке ошибки и это превратит данное всплывающее меню в постоянно действующее и позволит вам скопировать данное сообщение об ошибке:



Если вы обнаружите некое сообщение подобное Get value from agent failed: cannot connect to [[192.168.1.100]:10050]: [111] Connection refused (скорее всего с другим IP

адресом), это означает, что ваш сервер Zabbix не смог подключиться к такому порту демона агента. Это может происходить по целому ряду причин, наиболее частой из них является межсетевой экран - либо некий сетевой между вашими сервером Zabbix и удалённым хостом, либо некий локальный в самом удалённом хосте. Убедитесь что разрешено подключение с вашего сервера Zabbix к подлежащей отслеживанию машине по порту 10050. Если вы наблюдаете нечто подобное тому что было отображено в нашем предыдущем снимке экрана с no route to host, тогда вы скорее всего допустили ошибку при настройке и ваш сервер Zabbix не может подключиться к данному хосту с его агентом Zabbix.

Если вы всё сделали верно (или если у вас нет некого межсетевого экрана, блокирующего это подключение), вы могли бы снова пройти в Monitoring | Latest data - только это опять же было бы бессмысленным. Чтобы посмотреть почему освежите список хостов. Вскорости вы должны обнаружить, что иконка состояния этого агента Zabbix вновь окрасится красным, вам следует поместить на неё курсор мыши чтобы обнаружить другое сообщение об ошибке, Received empty response from Zabbix Agent at [192.168.1.100], что предполагает, что ваш агент сбросил данное подключение по причине полномочий доступа. Теперь всё иначе. О каких полномочиях идёт речь и почему всё работало для нашего первого хоста?

Со своего сервера Zabbix выполните следующее (замените IP адрес правильным для вашего хоста):

Замените IP адрес адресом своего удалённого хоста. Вы должны увидеть следующий вывод и ваше подключение должно немедленно закрыться:

```
Trying 192.168.1.100...
Connected to 192.168.1.100.
Escape character is '^]'.
Connection closed by foreign host.
```

Теперь попробуйте то же самое в отношении localhost:

```
$ telnet localhost 10050
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'
```

Обратите внимание, что на этот раз соединение не закрывается сразу, следовательно, существует отличие. Данное подключение скорее всего будет закрыто слегка позднее - тремя секундами позже, что может быть весьма особым. Если это не произойдёт по какой- то причине, нажмите, как и предписано, Ctrl +], а затем введите quit - это должно закрыть данное соединение:

```
^]
telnet> quit
Connection closed.
```

Как оказалось, настройка демона агента Zabbix на другой машине будет слегка сложнее чем раньше.

В отличие от установке на самом сервере Zabbix нам придётся внести изменения в файл настроек этого демона агента на данной удалённой машине. Откройте в предпочитаемом вами редакторе zabbix_agentd.conf от имени root и отыщите параметр Server. В настоящее время он настроен на 127.0.0.1, что и является той причиной, по которой мы не способны общаться с ним со своего сервера Zabbixю Как постулирует соответствующий комментарий, этот параметр должен содержать IP адрес вашего сервера Zabbix, поэтому замените здесь 127.0.0.1 на верный адрес своего сервера Zabbix.

Сохраните этот файл и перезапустите этот демон агента. Как именно это сделать, опять же, зависит от вашего способа установки. Если она выполнялась из пакетов распространения, следующее скорее всего должно сработать:

```
# systemctl restart zabbix-agentd
```

Если вы устанавливали из исходного кода и не создавали или не приспосабливали некий сценарий init, вам придётся вручную остановить и запустить этот процесс агента:

```
# killall -15 zabbix_agentd; sleep 3; zabbix_agentd
```

Наша предыдущая команда остановит все процессы с названием zabbix_agentd в данной системе. Её не следует применять если в такой системе запущено множество агентов. Кроме того, установленной задержки в 3 секунды должно быть более чем достаточно в большинстве случаев, но если ваш агент не будет запущен после этого, проверьте его файл журнала для потенциальных причин. Также имеется возможность, что вам придётся определить само местоположение этого исполняемого файла zabbix_agentd если этот файл не находится в вашем пути, например, /usr/bin/zabbix_agentd.

Для проверки изменений попробуйте снова подключится telnet -ом к своей удалённой машине:

```
$ telnet 192.168.1.100 10050
```

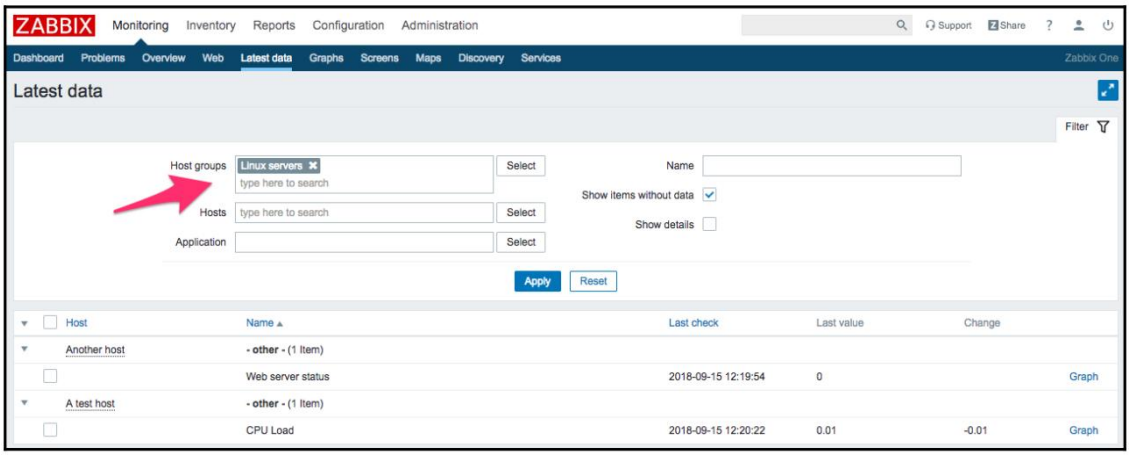
В этот раз результат должен быть таким же как и для локального хоста - это подключение должно открыться и затем закрыться примерно через три секунды.

Наконец, стоит открыть Monitoring | Latest data. Однако мы увидим только свой ранее созданный элемент; причина кроется в том самом фильтре, который мы меняли ранее. Мы в явном виде фильтровали только один хост; следовательно, второй созданный нами хост вовсе не отображается.

В этом фильтре, который всё ещё должен быть раскрыт, очистите соответствующее поле хоста и выберите Linux servers в поле Host groups, а затем кликните по Apply.

Во многих полях фильтров Zabbix мы можем либо начать набирать и получить некий список соответствующих записей, либо кликнуть по кнопке Select чтобы просмотреть перечень всех доступных логических объектов. Набор является очень удобным способом когда мы знаем по крайней мере часть нужного названия. Возможность посмотреть весь список полезна при работе в некоторой среде когда она нам менее знакома.

Теперь мы должны наблюдать два отслеживаемых хоста, причём каждый из них имеет по одному элементу:



Заметим, что мы можем кликнуть по треугольной иконке вслед за каждой из записей или по соответствующему заголовку длЯ свёртывания и раскрытия либо некоторой индивидуальной записи, либо всех имеющихся записей.

Клонирование элементов

Давайте теперь выполним мониторинг другой службы, например, той, которая запускается по порту 22, SSH:

Чтобы всё сделать по- простому, мы не желаем на этот раз создавать некий элемент с нуля; вместо этого вернитесь обратно к Configuration | Hosts.

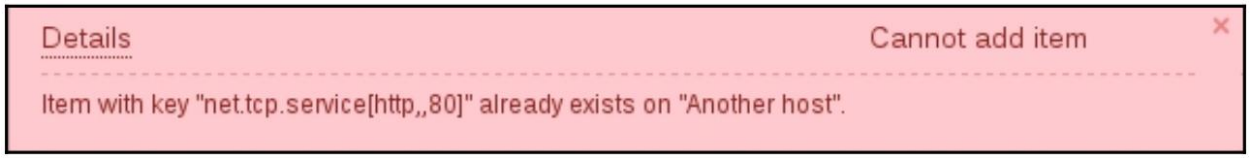
Кликните по Items вслед за Another host.

Кликните по Web server status в колонке Name. Это открывает соответствующий экран изменения элемента, показывая все введённые нами ранее значения.

В этот раз в самом низу существуют доступными различные кнопки. Помимо прочих изменений, вместо кнопки Add теперь имеется Update.

Существует также и Delete, которая, очевидно, удаляет открытый в данный момент элемент. Мы не желаем делать этого сейчас. Вместо этого нажимаем на Clone.

Обратите внимание как эта открытая форма предлагает создавать новый элемент, ибо в данном случае все значения настроены теми же самыми что и в первоначальном элементе который мы должны клонировать. Наша кнопка Update также изменена на Add. Кликните по Add и вы должны получить отказ. Помните, мы говорили о том, что ключ предполагается уникальным в каждом хосте; именно об этом и говорит сообщение об ошибке:



Наш изменяемый элемент всё ешё открыт, поэтому мы можем исправить свою ошибку. Выполните следующие изменения:

Name: Измените на SSH server status

Key: Измените http,,80 на ssh, стем чтобы он выглядел как net.tcp.service[ssh]

Это всё что нам требовалось сделать сейчас, поэтому кликните по кнопке Add в самом низу снова. На этот раз данный элемент должен быть успешно добавлен. Теперь перейдите в Monitoring | Latest data, где Another host должен иметь перечисленными два элемента - SSH server status и Web server status. Их состояние будет определяться тем какая служба запущена в нашем удалённом хосте. Поскольку он удалённый, SSH скорее всего запущен (и следовательно имеет значение 1), однако будет ли запущен веб сервер, целиком зависит от вашей ситуации. Имейте в виду, что может пройти несколько минут,

прежде чем вы получите самое первое значение в имеющихся последних данных для своего нового элемента:

Опрос элементов вручную

Добавление элементов в своём интерфейсе и ожидание обновления элемента является одним из способов посмотреть получил ли ваш элемент верный ключ. Это не очень быстрый метод, однако - вам придётся ждать проверки сервером данного элемента. Если вы не уверены в определённых параметрах или же хотели бы проверить иную комбинацию, самым простым способом выполнения этого является проверка утилитой с названием zabbix_get. При установке из исходного кода он устанавливается вместе с самим агентом Zabbix. При установке из пакетов он может быть установлен совместно с агентом Zabbix, лиюо может поставляться в отдельном пакете. Его применение очень простое: если мы желаем выполнить запрос своего агента с имеющегося сервера Zabbix, мы запустим его на своём сервере Zabbix, некий test host.

В Debian/Ubuntu выполните такую команду:

apt install zabbix-get

Red Hat/Centos запустите следующую команду:

yum install zabbix-get

Вот та команда, которую следует запустить в оболочке нашего сервера Zabbix

$ zabbix_get -s 127.0.0.1 -k system.cpu.load

Она получит своё значение в точности тем же образом, как если бы это делал наш сервер. Если вы желаете получать подобные этим значения от другого хоста, вы можете запустить zabbix_get на самом сервере Zabbix. Попытка запустить его в том же самом хосте, на котором исполняется данный агент завершится отказом, поскольку мы изменили имеющийся параметр Server на приём соединений только от своего сервера Zabbix. Если вы желали бы опрашивать своего агента с локального хоста для целей отладки, в параметр Server можно добавить 127.0.0.1 через запятую - это иногда делается во всех системах при развёртывании его агента. Параметр -s служит для определения соответствующего IP/имени хоста для такого хоста, а -k для задания значения ключа элемента, как мы его определяли в Zabbix для своего элемента. Для проверки всех имеющихся параметров, которые вы можете применять, исполните zabbix_get --help.

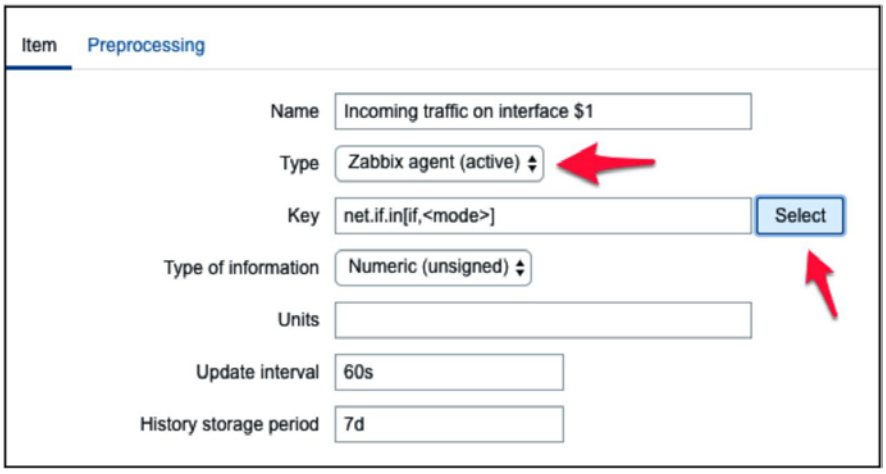
Это завершает основы обычных, или пассивных элементов Zabbix, когда сами серверы опрашивают агентов. Давайте перейдём к прочим типам элементов.

Активные элементы

Пассивные элементы Zabbix это прекрасно когда вы можете подключаться ко всем отслеживаемым хостам с самого сервера Zabbix, но что если вы не можете разрешать входящие подключения к подлежащим мониторингу хостам по причинам безопасности или сетевой топологии?

Здесь на поле выходят активные элементы. В противоположность пассивным элементам, что касается активных элементов, именно сам агент подключается к своему серверу; сам сервер никогда не подключается к такому агенту. При подключении этот агент выгружает перечень элементов для проверки и затем периодически выдаёт отчёт о своих новых данных соответствующему серверу. Давайте создадим некий активный элемент, но на этот раз мы попытаемся воспользоваться некоторой помощью при выборе соответствующего ключа:

Перейдите к Configuration | Hosts
Кликните по Items вслед за Another host
Кликните по Create item
В этот раз мы применим такие значения:
Name: Incoming traffic on interface $1
Type: Zabbix agent (active)
Update interval: 60s
History storage period: 7d



На этот раз мы делаем нечто иное со своим полем Key.

Кликните по кнопке Select и в возбуждённом диалоге, который мы уже наблюдали ранее, кликните по net.if.in[if,<mode>]. Это заполнит выбранную вами строку следующим образом:

Если в вашей системе имеются сетевые интерфейсы с различными названиями, применяйте их вместо eth0. Вы можете выявит свои названия интерфейсов с помощью команд ifconfig или ip addr show. Во многих современных дистрибутивах ранее стандартная схема именования ethX была заменена на схему, которая в результате приводит к различным именам интерфейсам, таким как enp0s3 и em1. Далее замените все вхождения eth0 на правильное название своего интерфейса:

Перейдите к Monitoring | Latest data и проверьте появятся ли новый значения.

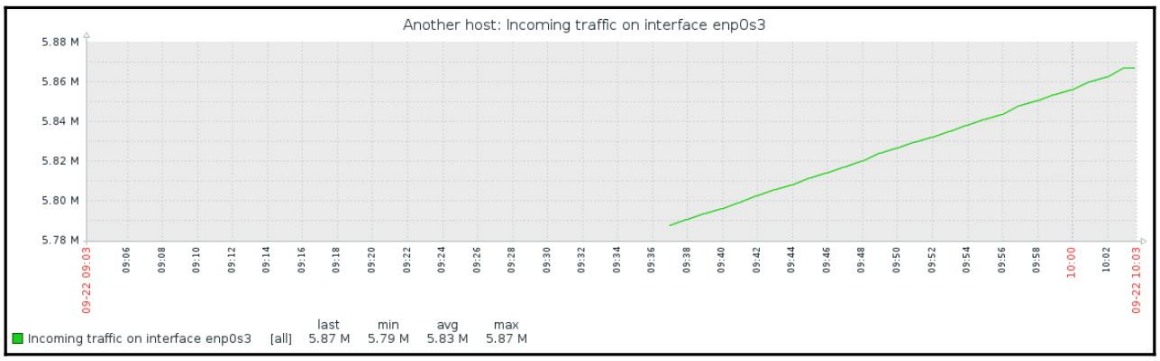
Ну, как- то не похоже что они появились. Вы можете подождать ещё немного, чтобы окончательно убедиться в этом, но скорее всего данные для нового активного элемента не возникнут, а это означает, что мы перешли к следующей серии устранения неполадок.

Во- первых, нам следует проверить базовую сетевую связь. Помните, активные агенты подключаются к своему серверу, поэтому нам следует знать какой порт они используют (по умолчанию это порт 10051). Поэтому давайте начнём с проверки того может ли удалённо отслеживаемая машина подключаться к своему серверу Zabbix:

Отметим что данная система в приводимом снимке экрана в действительности обладает интерфейсом enp0s3, а не eth0. Мы обнаружим как Zabbix заботится о названиях интерфейсов и автоматически их обнаруживает в Главе 11, Автоматизация настройки.

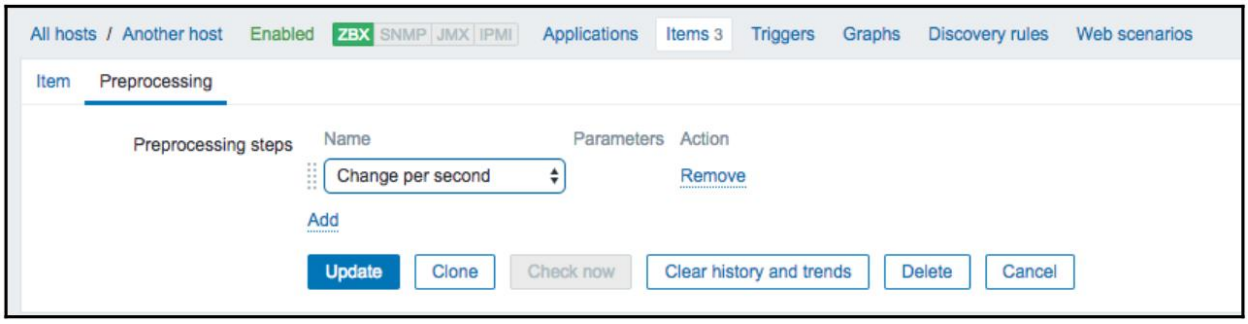
Если вы не наблюдаете никаких данных и соответствующий элемент отображается как не поддерживаемый в имеющемся разделе настроек, проверьте название этого интерфейса.

Великолепно, данные в конце концов потекли, но значения выглядят очень странно. Если вы немного подождёте, вы обнаружите, что отображаемое в колонке Last Value просто продолжает увеличиваться. Итак, в чём дело? Хорошо, ключи сетевого обмена получают свои данные из счётчиков интерфейса, то есть ваш сетевой интерфейс добавляет весь обмен, и именно этими данными запитывается имеющаяся в Zabbix база данных. Это имеет одно большое преимущество - даже когда опрашиваемые данные имеют большие интервалы скачки обмена не останутся незамеченными при наличии данных соответствующего счётчика, но это также делает для вас данные в значительной степени плохо читаемыми, а графики будут выглядеть как постоянно растущая линия (если хотите поглядеть каково это, кликните по ссылке Graph для данного элемента). Мы даже можем обозвать его графиком горы:



К счастью, Zabbix предоставляет встроенную возможность иметь дело с подобные таким счётчикам:

- Перейдите к Configuration | Hosts
- Кликните по Items вслед за Another host
- Кликните по Incoming traffic on interface eth0 в соответствующей колонке Name
- Перейдите к закладке Preprocessing и измените Preprocessing steps на Changes per second
- Кликните по Update



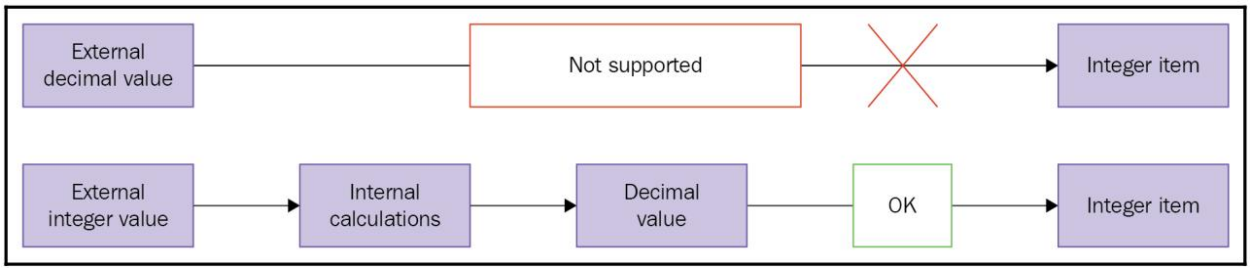
Нам придётся слегка подождать пока наши изменения вступят в силу, поэтому сейчас лучшее время для обсуждения нашего выбора параметра Type of information для данного элемента. Мы установили его в Numeric (unsigned), что принимает целые значения. Значения для данного элемента первоначально в действительности являются целыми - это значения счётчиков, обозначающие число байт, получаемых в данном интерфейсе. Наш параметр Preprocessing steps был изменён на Changes per second (в

предыдущих версиях Delta speed per second)), тем не менее, почти всегда это приводит к появлению некоторой десятичной части; это делит значение общего обмен между двумя значениями на значение секунд, прошедших между ними. В тех случаях, когда Zabbix получает некое десятичное число и должен сохранять его в поле с целочисленным значением, его поведение будет отличаться в зависимости от того каким он образом он получил данное десятичное значение так:

Если это десятичное значение получается из некоторого источника агента Zabbix, такого как system.cpu.load, такой элемент окажется не поддерживаемым

Если Zabbix получает некое целое, но последующие вычисления в результате приводят к появлению десятичного числа, как в случае с нашим сетевым элементом, его десятичное значение будет отбрасываться.

Данное поведение отображается на следующей схеме:

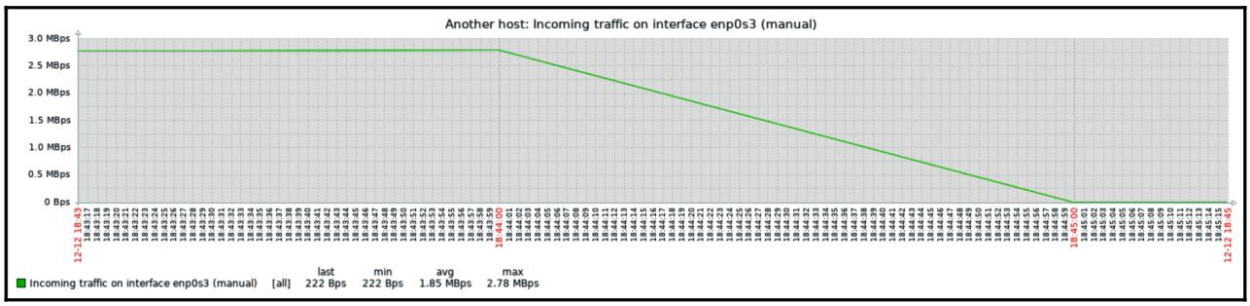


Почему имеется подобное отличие и почему мы оставляем данный элемент неким целым, раз это приводит в конечном результате к меньшей точности? Десятичные значения в применяемой в Zabbix схеме базы данных имеет меньшее число значимых цифр, доступных перед десятичной точкой, чем у целых значений. Для нагруженных интерфейсов с высокой скоростью мы можем переполнять этот предел и это повлекло бы к полной утрате получаемого значения. Обычно лучше будет потерять небольшую часть точности - десятичную часть - чем утратить всё значение. Отметим, что теряется точность в самом меньшем элементе: байте или бите. Даже если Zabbix показывает 5 Gbps в своём интерфейсе, его отсекаемая десятичная часть будет значением в битах; следовательно, такая утрата точности на самом деле должна быть очень незначительной. Предлагается применять целые значения для элементов у которых имеется подобный обсуждённому риск, по крайней мере пока пределы схемы базы данных не возрастут.

Проверьте вновь Monitoring | Latest data и вы обнаружите что изменяющееся число является отрицательным, покольку мы теперь рассчитываем изменение в секунду вместо постоянно увеличивающегося значения. Следовательно, получаемое нами значение скорее всего будет меньше чем в прошлый раз.

Имейте в виду, что в наихудшем случае изменения конфигурации могут занимать до трёх минут чтобы быть переданными данным агентом Zabbix - одна минута для достижения настроек кэша сервера и две минуты пока сам агент не обновит свой собственный список элементов. Помимо такой задержки, данный элемент отличается от прочих созданных нами - он должен получать два значения для вычисления значения в секунду, которое именно и представляет наш интерес; следовательно, нам также придётся подождать какой бы интервал времени не прошёл ранее пока самое первое значение появится в нашем веб интерфейсе.

Так- то лучше; Zabbix теперь автоматически вычисляет изменение между каждыми двумя проверками (именно этому и служит дельта) и сохраняет его, но значения всё ещё не кажутся слишком дружественными для пользователя. Может быть они будут лучше на своём графике - давайте откроем соответствующую ссылку Graph чтобы узнать об этом:



Ух. Хотя мы очевидно можем видеть вступившие в действие сделанные изменения, но это всё же оставляет нас с очень корявыми историческими данными. Ось Y- этого графика представляет значение полного счётчика (а следовательно общее значение с начала отслеживания системой), однако наша ось X- предоставляет правильные данные (дельта). Вы также можете просматривать эти данный в численном виде, переходить к ниспадающему меню в правой верхней части, которая в настоящий момент считывает Graph. Выберите здесь 500 latest values. Вы получите следующий снимок экрана:

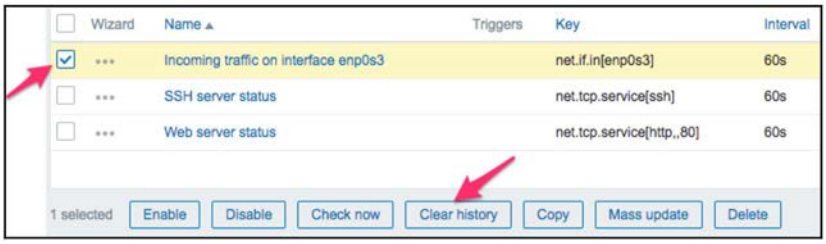
Timestamp	Value
2018-12-12 18:46:30	249
2018-12-12 18:46:00	216
2018-12-12 18:45:30	254
2018-12-12 18:45:00	222
2018-12-12 18:44:00	2917670
2018-12-12 18:43:30	2910581
2018-12-12 18:43:00	2902951
2018-12-12 18:42:30	2896697
2018-12-12 18:42:00	2889398

В этом спсике мы можем прекрасно видеть сами изменения в представлении данных, а также точное время когда это изменение было выполнено. Но эти гигантские значения поступают к нам из наших счётчиков данных и они переполняют наш милый, ясный график, обладая слишком крупным масштабом - нам придётся избавиться от них:

Проследуйте в Configuration | Hosts

Кликните по Items вслед за Another host

Пометьте фаг вслед за элементом Incoming traffic on interface enp0s3 (или какой там ещё у вас интерфейс) и взгляните на те кнопки, которые расположены внизу списка данного элемента:

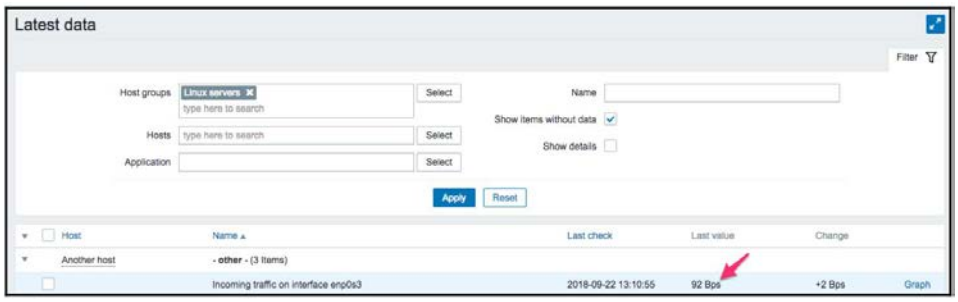


Четвёртая слева кнопка с названием Clear history, скорее всего, делает то что нам нужно. Отметим текст 1 selected слева от кнопок активности - он отображает общее число выбранных элементов, поэтому мы всегда знаем к какому числу элементов мы применяем действие. Кликните по кнопке Clear history. Вы должны получить всплывающий вопрос JavaScript относительно подтверждения на продолжение. Поскольку очистка истории может занять много времени для больших наборов данных, в нашем случае это должно произойти почти моментально, поэтому кликните по кнопке OK. Это должно избавить нас от всей истории значений для данного элемента, включая наши гигантские.

Тем не менее, глядя на ось Y на данном графике, мы видим, что поступающие значения не сопровождаются никаким пояснением того что они представляют, а при больших значениях применяются K, M и прочие идентификаторы множителя. Было бы намного лучше, если бы Zabbix знал как вычислять это в байтах или подобных единицах:

1. Проследуйте в Configuration | Hosts
2. Кликните по Items вслед за Another host
3. Кликните по интерфейсу Incoming traffic on the enp0s3 (или какой там у вас интерфейс) в колонке Name. Измените поле Units и введите Bps
4. Кликните по Update

Давайте проверим есть ли какие- то улучшения в Monitoring | Latest data



Один установленный нами параметр, интервал обновления, мог бы быть поменьше, следовательно в результате он приводил бы к более представительному графику. Но важно помнить, что чем меньше интервал вы имеете для своих элементов, тем больше данных приходится получать Zabbix и, каждую секунду, больше данных вставляется в имеющуюся бызу данных и больше вычислений придётся выполнять при отображении таких данных. Хотя это может быть незаметной разницей для нашей тестовой системы; вам следует пытаться сохранять интервалы настолько крупными, насколько это возможно.

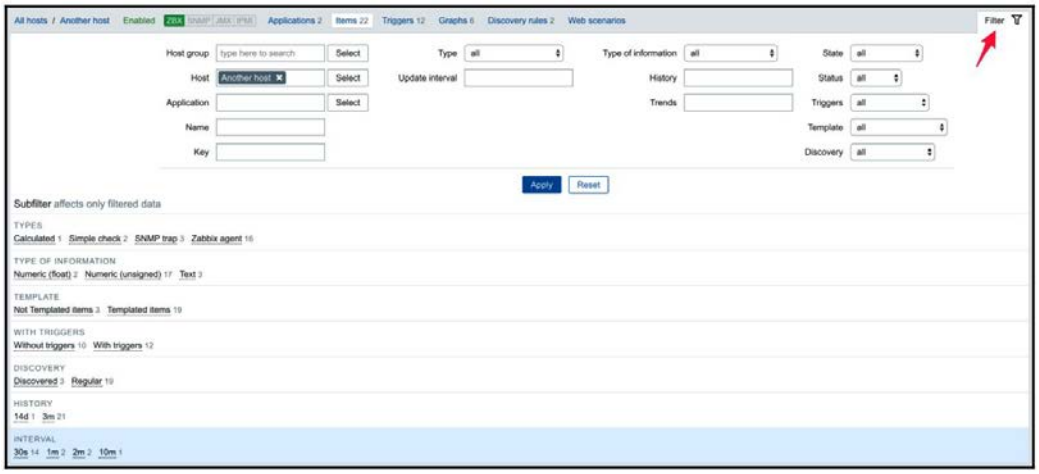
До сих пор мы создавали элементы, которые получали численные данные - либо целые, либо десятичные значения. Давайте создадим ещё один, слегка отличающийся на этот раз:

Как обычно, проследуйте в Configuration | Hosts

Кликните по Items вслед за Another host. Прежде чем мы продолжим создание элемента, давайте рассмотрим какие полезные вещи доступны в нашем разделе настроек, в частности, для элементов. Если мы взглянем поверх самого списка элементов, мы можем обнаружить полоски навигации и информации.

Эта область предоставляет быструю и полезную информацию относительно выбранного в данным момент хоста - его имя, является ли этот хост отслеживаемым и его доступность. Даже что ещё более важно, в правой верхней части они предоставляют быстрые закладки возврата к перечню хостов и прочим элементам, связанным с текущим хостом - приложениям, элементам, триггерам, графикам, правилам обнаружения и веб-сценариям. Это удобный способ переключения между категориями элементов для отдельного хоста без перехода каждый раз к списку хостов. Но это ещё не всё.

Кликните по кнопке Filter чтобы открыть тот фильтр, что мы получали поверх своей морды ранее. Вновь появится выразительный фильтр:



Активный агент со множеством серверов

При том способе, которым мы настроили ServerActive в файле настройки демона агента, он подключается к отдельному серверу Zabbix и отправляет данные элементов в этот сервер. Некий агент также способен работать со множеством серверов одновременно; нам только придётся определить дополнительные адреса здесь в виде разделённого запятыми списка. В таком случае наш агент будет внутренне порождать индивидуальные процессы для индивидуальной работы с каждым сервером. Это означает, что один сервер не будет знать о том, что мониторинг выполняет и иной сервер - значения будут отправляться каждому из них независимым образом. С другой стороны, даже если некоторые серверы запрашивают данные индивидуальных элементов, эти данные будут собираться несколько раз, по разу для каждого сервера.

Совет

Всегда проверяйте комментарии в файлах настройки; они могут быть крайне полезными. В случае ServerActive соответствующий комментарий показывает, что агент также может подключаться к не определённым по умолчанию портам в каждом из серверов применяя синтаксис, подобный server1:port или server2:port.

Работа со множеством серверов в активном режиме может быть полезной в случае при миграции с одного экземпляра Zabbix на другой. На некоторое время какой- то из агентов может выдавать отчёты обоим серверам, и старому, и новому. Ещё одним случаем когда это будет полезно, это когда некая среда пользователя, в которой этот пользователь может иметь некий локальный сервер, который выполняет полностью законченный мониторинг, в то время как некая внешняя компания может пожелать отслеживать лишь некоторые стороны относительно доставляемых ими приложений.

Для пассивных элементов допуск входящих подключений со множества серверов Zabbix выполняется тем же самым образом - путём добавления множества IP адресов в соответствующий параметр Server.

Поддерживаемые элементы

Мы создали некие элементы, которые применяют Zabbix в обоих направлениях и собирают данные. Но это не единственные доступные элементы. Вы можете ознакомиться с полным списком при создании какого- то элемента вновь (проидите в Configuration | Hosts, кликните по Items для любого из хостов и затем кликните по кнопке Create item после кнопки Select, следующей за соответствующим полем Key) чтобы посмотреть какие элементы встроены для агентов Zabbix с кратким описанием для большей части из них.

Замечание

Не все элементы агента Zabbix доступны как в виде пассивных, так и в виде активных элементов. Например элементы log и event log (для получения информации файла журнала и журнала событий Windows, соответственно, доступны только в качестве активных элементов). Мониторинг журнала рассматривается в Главе 10, Расширенный мониторинг элемента, а относящиеся к специфике Windows элементы в Главе 22, Мониторинг Windows.

Рассматривая данный список, мы можем видеть какие категории элементов агенты Zabbix поддерживают естественным путём - настройку системы, сетевой обмен, сетевые службы, загруженность системы и использование памяти, мониторинг файловой системы и прочее. Но это не означает, что всё что вы видите будет работать в любой системе в которой исполняется демон агента Zabbix. Поскольку каждая платформа имеет свой отличный способ выставления такой информации и некоторые параметры могут оказаться специфичными для этой платформы, нет гарантии что все ключи будут работать во всех хостах.

Например, когда для userspace изменяется отчёт определённой статистики дискового устройства, имеющийся агент Zabbix должен особым образом реализовывать поддержку для такого нового метода, причём более ранние версии будут поддерживать меньшее число параметров имеющихся в настоящий момент систем Linux. Если вам интересно будет ли определённый параметр работать в конкретной версии особой операционной системы, наилучшим способом будет ознакомиться с соответствующим руководством Zabbix, а затем проверить его. Вот некотороые из наиболее часто применяемых ключей элементов агента:

agent.ping: Возвращает 1 когда данный агент доступен и ничего совсем когда этот агент не доступен

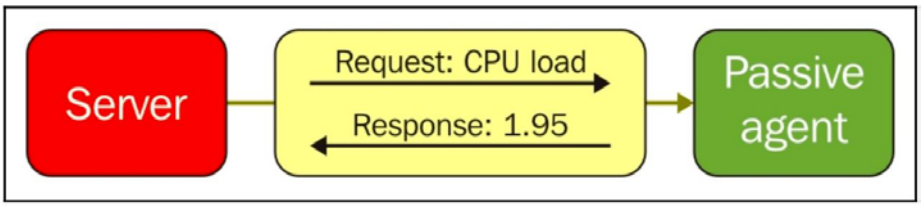
- net.if.in/out/total: Предоставляет информацию и входящем/ исходящем или общем обмене
- net.tcp.service: Пробует осуществить простейшее подключение к некоторой службе TCP
- proc.num: Исчисляет общее число процессов и может фильтроваться различными параметрами
- vfs.fs.size: Предоставляет информацию об использовании файловой системы
- vm.memory.size: Предоставляет информацию о применении памяти
- system.cpu.load: Предоставляет информацию о загрузке ЦПУ в стандартном десятичном представлении
- system.cpu.util: Предоставляет информацию об использовании ЦПУ, например, iowait

Для большей части из них могут быть указаны различные параметры для фильтрации результатов или выбора конкретной части информации. К примеру, proc.num[,zabbix] будет исчислять число всех процессов, которые запущены соответствующим пользователем Zabbix.

Выбор между активными и пассивными элементами

Хотя мы и обсуждаем агенты Zabbix в качестве активных или пассивных, некий агент на самом деле не является тем или иным - само направление коммуникации определяется на уровне его элемента. Некий агент способен (и при определении по умолчанию делает это) работать в обоих режимах в одно и то же время. Тем не менее, мы будем вынуждены выбирать какой именно тип элемента применять - активный или пассивный. Говоря кратко - рекомендуется применение активных элементов.

Чтобы понять почему, давайте сопоставим как осуществляется такое подключение. В случае пассивного агента это очень просто:



Аудит файловой системы: как контролировать доступ к файлам и папкам и защищаться от утечек информации

В компании произошел неприятный инцидент – в общем доступе оказалась справка о здоровье одного из топ-менеджеров. Эта ситуация заставила начать разбираться: как такое могло произойти? К какой еще информации имеют доступ посторонние? Как далеко уходят документы? На каких компьютерах без учета и внимания хранятся персональные данные, «файлики» с паролями, документы с грифом «комтайна»? Какие неучтенные копии черновиков приказов выходят за пределы круга доверенных лиц?

С такими вопросами компания ставила на тест FileAuditor, российскую DCAP-систему разработки «СёрчИнформ». Нужно отметить, что и до установки решения Data-Centric Audit and Protection (DCAP) заказчик не игнорировал вопрос защиты файловой системы. Аудит обращения к файлам пытались делать средствами операционной системы в связке с системами анализа логов. Но стало очевидно, что при существующем объеме файлов и папок «подручными» средствами уже не обойтись, да и нагрузка на файловые серверы оказывалась слишком высокой.

Решили попробовать специализированную систему и поставили перед ней конкретные задачи. Программное обеспечение должно:

- Делать «уборку»: сканировать всю файловую систему, проверять документы по политикам безопасности. Если документ соответствует заданной в политике безопасности категории, ему присваивается метка – какого типа эти данные (персональные, коммерческая тайна, номера банковских карт и так далее).
- Отслеживать все операции, которые производят с этими файлами: кто создал, отредактировал, переместил, удалил.
- Проводить аудит прав доступа, то есть автоматически отслеживать: какие файлы каким пользователям доступны.
- Блокировать неправомерные действия пользователей с файлами. Это уникальный функционал «FileAuditor СёрчИнформ», благодаря которому программа не просто приводит файловую систему в порядок, но и обеспечивает полную защиту «данных в покое».
- Архивировать критичные документы, чтобы расследовать инциденты и восстанавливать потерянную информацию.

Спойлер: FileAuditor со всеми задачами справился, и клиент закупил лицензии. Но давайте рассмотрим функционал подробнее.

Сканирование файловых хранилищ

FileAuditor ведет непрерывный мониторинг файлов и папок, чтобы оперативно выявлять изменения в них.

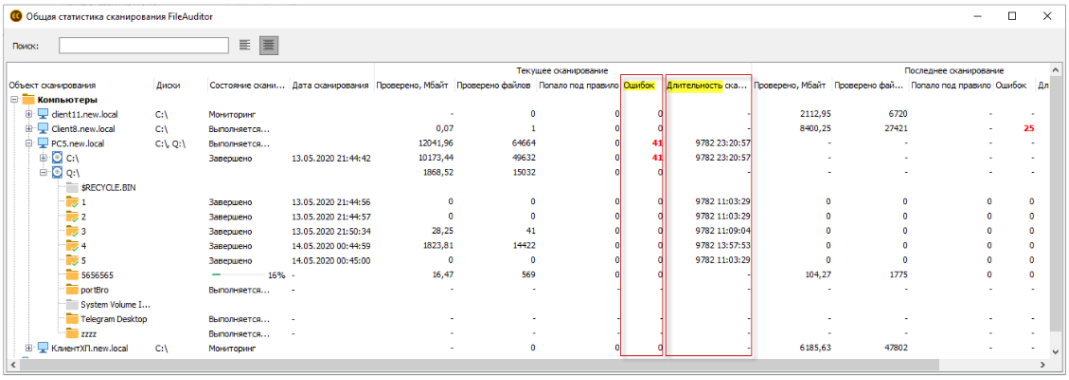
При первом сканировании программа вычитывает всю структуру и содержимое файлов на контролируемых компьютерах. В дальнейшем в первую очередь система будет сканировать те файлы и папки, к которым обращались пользователи – открывали, редактировали, удаляли, создавали новые, переименовывали или перемещали. Причем

изменения на ПК сотрудников отслеживаются в реальном времени, то есть ИБ-специалист всегда имеет актуальное представление о происходящем с данными в компании.

Агенты FileAuditor незаметны для пользователей, не тормозят контролируемые машины благодаря настройкам:

- расписания проверок (например, только по окончании рабочего времени);
- условия проверок (например, только если загрузка ЦП меньше N%, только в отсутствии активных сессий и т.д.);
- скорости сканирования (ее можно снизить для облегчения нагрузки на инфраструктуру).

Чтобы еще сэкономить время и ресурсы можно исключить из сканирования некоторые документы и папки. Например, это нужно сделать с системными файлами.

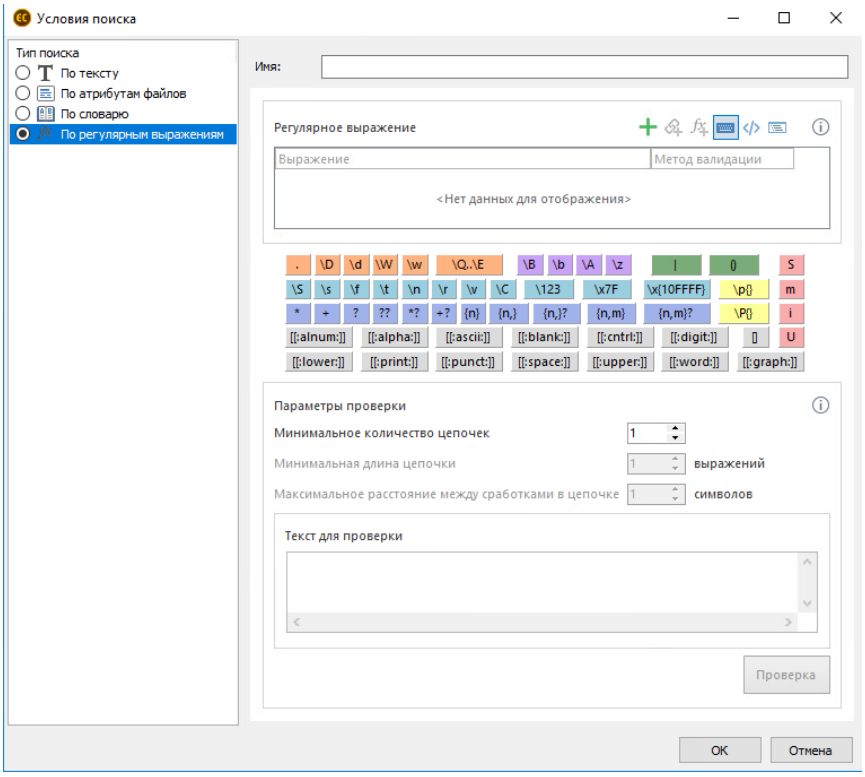


Классификация данных

В отличие от традиционных средств контроля файловых систем, FileAuditor классифицирует файлы не только по названию или расположению, но и по содержимому файлов: делит их на категории и выделяет среди них конфиденциальные. Это делается по предварительно заданным правилам классификации: какими признаками должен обладать файл, чтобы попадать в ту или иную категорию.

Искать эти признаки программа может:

- По ключевым словам, фразам и последовательности символов (иноязычные вставки, @, №, $, % и т.д.). Поддерживается поиск ключевых слов с морфологией, т.е. в измененных формах. Можно уточнить поиск, указав, сколько раз в документе должны встречаться искомые слова и фразы. Если искать сразу несколько ключевых слов, можно задать, какое расстояние в документе между ними допустимо, чтобы считать сочетание значимым.
- По словарям. В программе есть встроенный редактор, который автоматически преобразует в готовый словарь любой текст-образец, загружаемый пользователем. Этот вид поиска полезен для выделения тематических категорий документов: например, считать файл попадающим в категорию «финансовые документы», если в нем встретилось не менее 5 выражений из словаря бухгалтерской терминологии.
- По регулярным выражениям. Можно создавать сложные регулярные выражения, когда в одном поиске скомбинированы несколько условий. Например, учитывать в правиле классификации только файлы, где одновременно встречаются не менее 5 комбинаций из номеров карты и трехзначных CVC/CVV-кодов. Кроме того, можно сразу убедиться, что запрос работает корректно: доступно поле проверки, где можно задать пример искомой комбинации символов и протестировать, распознает ли его система.
- По атрибутам. Критерий позволяет относить к правилу классификации только файлы определенного типа, размера, созданные или измененные в заданном интервале, хранящиеся в определенной директории и т.д.



Архивирование критичных документов

FileAuditor создает теневые копии файлов, чтобы защитить документы от несанкционированных изменений, удаления.

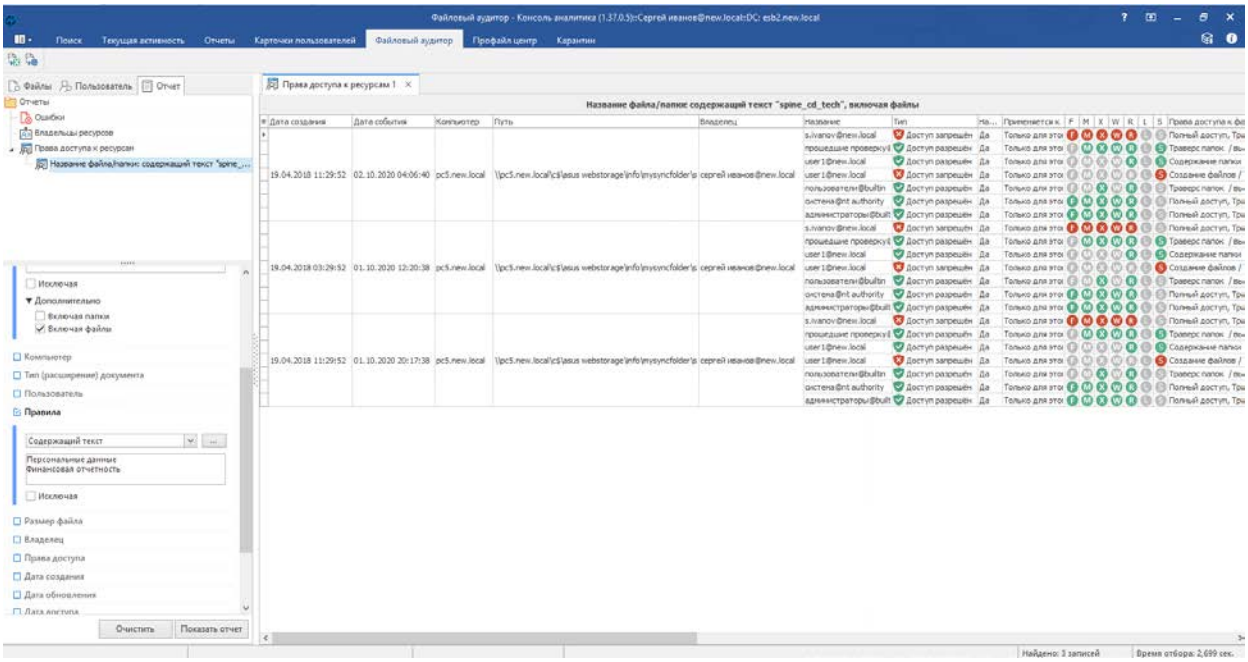
Сервер не будет перегружен копиями лишних файлов, так как можно настроить, копии каких документов нужно сохранить. Реализована и система дедупликации (идентичные копии будут удаляться), есть настройка, чтобы устаревшие копии, с которыми пользователи перестали взаимодействовать, автоматически удалялись из выдачи. То же и копиями файлов, которые больше не нуждаются в контроле и исключены из мониторинга.

Аудит прав доступа

- FileAuditor определяет права доступа пользователей к каждому документу благодаря вычитке сведений из ресурсов файловой системы. Программа видит:
- перечень групп и конкретных сотрудников, которым доступен файл;
- перечень операций, доступных каждому пользователю с конкретным файлом/директорией.

В программе есть фильтры, которые помогают конкретизировать выдачу для более детального анализа прав доступа. Для каждого файла можно найти всех пользователей с определенными разрешениями.

Например, вы можете выбрать перечень всех сотрудников, кто может редактировать и удалять файл, или только тех, кому доступ к файлу запрещен. И наоборот: можно искать, какие файлы доступны или запрещены к использованию заданным пользователям/группам пользователей.

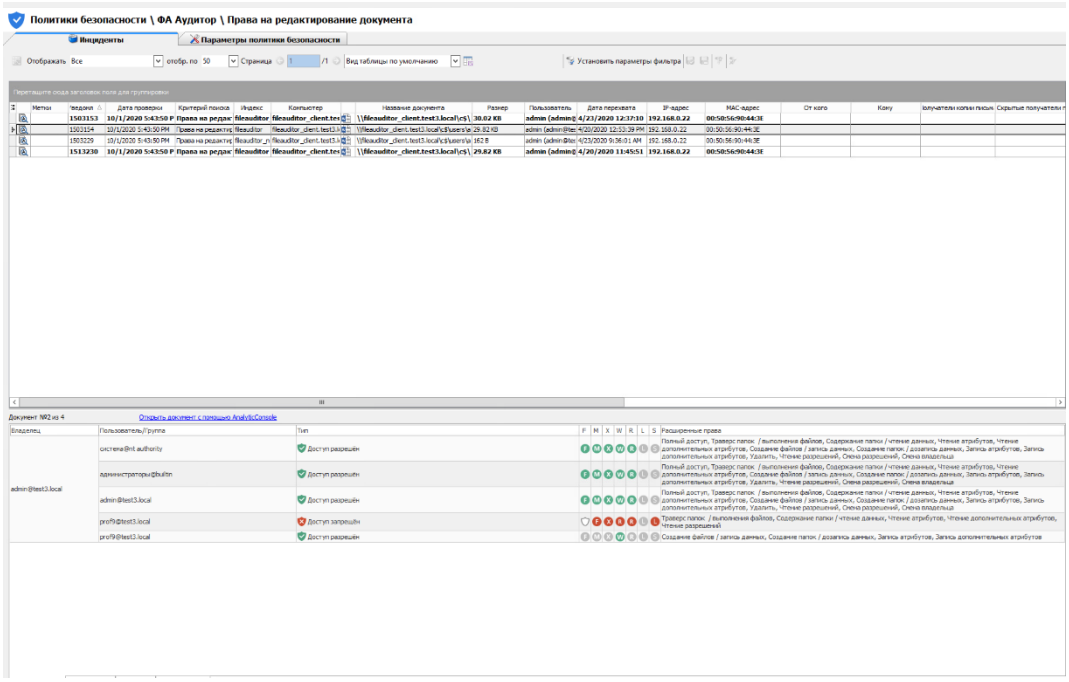


Управление инцидентами

Политики безопасности в FileAuditor помогают вовремя среагировать на нежелательные события с заданными категориями данных. Настроить автоматизированный поиск нарушений можно:

- по категории файла или папки (в соответствии с правилами классификации);
- по расположению;
- по типу;
- по расширению;
- по пользовательским правам доступа;
- по дате создания или изменения и т.д.

Например, можно создать политику, которая оповестит, если новые пользователи получили расширенные права доступа к документам из категории «Финансовая отчетность». Или если с документа снят гриф «коммерческая тайна».



Блокировка по меткам как возможность защитить файлы

В FileAuditor реализованы блокировки по меткам – возможность запрещать доступ и пересылку конфиденциальных файлов в любых произвольных приложениях.

Например, в FileAuditor можно запретить отправку файлов с меткой «ПДн» по любому каналу – будь то корпоративный мессенджер или Telegram. Пользователь просто не сможет прикрепить такие документы во вложения и получит уведомление об ошибке. Можно разрешить работу в MS Office с документами из категории «Конфиденциально» только директору – тогда все остальные пользователи, даже получив доступ к такому файлу, не смогут его открыть.

Метки незаметны для пользователей и наследуются при различных действиях с файлами, включая копирование, переименование, смену расширения. FileAuditor автоматически перепроверяет наличие меток и устанавливает их на вновь создаваемые на базе конфиденциальных документов файлы. Это обеспечивает непрерывный контроль.

Огромное значение метки имеют для работы DLP, их наличие позволяет системе обеспечить мгновенную блокировку утечек конфиденциальных данных, потому что теперь защитной системе не нужно проверять содержимое каждого файла. Чтобы понять, насколько критичен документ, DLP теперь достаточно проверить его метку. Это еще и не перегружает систему. Блокировка по меткам реализована в DLP-системе «СёрчИнформ КИБ».

Преимущества «СёрчИнформ FileAuditor»

До появления «файлового аудитора» от «СёрчИнформ» выбор заказчиков состоял только из зарубежных решений. Как правило, они не устраивали по цене, были громоздки, плохо интегрировались с существующими решениями в парке защитных систем компаний.

Отечественный продукт. Если компания обрабатывает и хранит персональные данные, она в принципе не имеет право пользоваться иностранными DCAP-системами.

Доступность. FileAuditor доступнее зарубежных аналогов. Ключевые зарубежные DCAP-системы доступны только крупным корпорациям и не по карману другим заказчикам. Кроме того, многие зарубежные продукты более требовательны к ресурсам, громоздки, что находит отражение в нагрузке на кадры и затратах на железо.

Русскоговорящая техподдержка рядом. Если у заказчика возникнут вопросы во время разворачивания системы или при работе, скорость ответа имеет решающее значение. Клиенты «СёрчИнформ», знакомые с работой менеджеров внедрения, инженеров, техподдержки, отмечают работу наших специалистов как одно из ключевых преимуществ при выборе вендора.

Возможность интеграции. FileAuditor легко интегрируется с другими продуктами «СёрчИнформ», в первую очередь с DLP «СёрчИнформ КИБ». Как говорилось выше, это существенно повышает уровень защиты информации, т.к. обеспечивается защита не только данных «в покое» (с помощью FileAuditor), но и «в движении» (что отслеживает DLP).

Задание: Разработайте политику агентского мониторинга для работы с файлами.

Практическое задание № 28-30.

Тема: Работа с исключениями из перехвата.

Цель: изучение способов обнаружения ошибок времени выполнения с помощью исключений; изучение основных принципов обработки исключений в языке C++; знакомство со структурным управлением исключениями.

Практическая часть:

ОБРАБОТКА ИСКЛЮЧИТЕЛЬНЫХ СИТУАЦИЙ

Схема обработки исключений в C++

Понятие Исключения (Exception) введено для генерации в системе сообщения об ошибке. Например:

```
Struct Range_error

{

int i;

Range_error(int ii):i(ii) { }

};

Char to_char(int i)

{

if(i < numeric_limits<char>::min() ||

i > numeric_limits<char>::max()) throw Range_error(i);

return i;

}
```

Функция To_char() либо возвращает Char по числовому значению I, либо генерирует исключение Range_error. Основная идея состоит в том, функция, обнаружившая проблему, которую она не знает как решать, генерирует (Throw) исключение в надежде, что вызывающий (прямо или косвенно) модуль знает, что делать в этой ситуации. Функция, которая собирается обрабатывать ошибку, может объявить, что она будет Перехватывать (Catch) исключения данного типа. Например, для вызова To_char() и перехвата исключений, которые она может вызвать, можно написать:

```
Void f(int i)

{

try

{

char c = to_char(i);

// …

}
```

```
catch(Range_error)

{

cerr << “ проблема!”;

}

}
```

Конструкция

```
Catch(/*…*/) { /* … */ }
```

Называется Обработчиком исключений. Она может использоваться только сразу после блока, начинающегося с ключевого слова Try, или сразу после другого обработчика; Catch также является ключевым словом. В скобках находится объявление, которое используется аналогично объявлению аргументов функции. То есть, оно указывает тип объектов, которые могут быть перехвачены этим обработчиком, и (необязательно) присваивает имена перехватываемым объектам. Например:

```
Void g(int i)

{

try

{

char c = to_char(i);

// …

}

catch(Range_error x)

{

cerr << “ проблема!: to_char(” << x. i << “) ”;

}

}
```

Если код в Try-блоке, или код, вызываемый из него, генерирует исключение, будут проверяться обработчики этого блока Try. Если сгенерированное исключение имеет тип, указанный в одном из обработчиков, будет выполнен этот обработчик. В противном

случае обработчики игнорируются и Try-блок ведет себя как обыкновенный блок. Если исключение сгенерировано и ни один из Try-блоков не перехватил его, выполнение программы прекращается.

Обработка исключений в C++ в основном является методом передачи управления специальному коду в вызывающем модуле.

Как правило, в программе существует несколько возможных типов ошибок на этапе выполнения. Такие ошибки можно распределить между исключениями с различными именами. Предпочтительней определять типы исключений (это сводит к минимуму некоторые неоднозначности, связанные с их назначением) и не использовать встроенные типы.

Предположим, что имеется программа калькулятор, который должен обрабатывать две ошибки времени выполнения: синтаксические ошибки и попытку деления на ноль. Нет необходимости передавать какое-либо значение обработчику из кода, обнаружившего попытку деления на ноль, поэтому деления на ноль может быть представлено простым пустым типом:

Class Zero_divide { };

С другой стороны, обработчик скорее всего предпочел бы получать информацию о том, какого вида встретилась синтаксическая ошибка. Например:

```
Class Syntax_error

{

Public:

const char* p;

Syntax_error(const char* q) { p = q; }

};
```

Теперь можно разделить обработку этих двух исключений, добавив обработчики после блока Try. При генерации исключения выполнится соответствующий обработчик. По завершении обработки исключения управление передается за конец списка обработчиков:

```
Try

{

// …

}

Catch(Syntax_error se)

{

// обработка синтаксической ошибки
```

```
cerr << " Синтаксическая ошибка: " << se. p;

// …

}

Catch()

{

// обработка деления на ноль

cerr << " Деление на ноль";

}

Catch(…)

{

// обработка остальных ошибок

}
```

Также как и в функциях, многоточие «…» означает «любой аргумент», поэтому Catch(…) означает «перехват всех исключений». Такой неспециализированный блок Catch() обозначает способность обрабатывать не обслуженные предшествующими блоками исключения, поэтому он должен размещаться последним.

Иерархическое управление исключениями

Исключение является объектом некоторого класса, являющегося представлением исключительного случая. Код, обнаруживший ошибку, генерирует объект инструкцией Throw. Фрагмент кода выражает свое желание обрабатывать исключение при помощи инструкции Catch. Результатом throw является поиск подходящего Catch (в функции, которая непосредственно или косвенно вызывала функцию, сгенерировавшую исключение).

Часто исключения естественным образом разбиваются на семейства. Из этого следует, что наследование может оказаться полезным для структурирования исключений и помочь при их обработке. Например, исключения для математической библиотеки можно организовать следующим образом:

```
Class Math_err { };

Class Overflow : public Math_err { }; // переполнение сверху

Class Underflow : public Math_err { }; // переполнение снизу

Class Zerodivide : public Math_err { };// деление на ноль
```

Это позволяет обрабатывать любой Math_err, не заботясь о том, какое в точности исключение возникло. Например:

```
Void f()

{

try { /* … */ }

catch(Overflow)

{

// обработка Overflow или всех производных от Overflow

}

catch(Math_err)

{

// обработка любой Math_err, не являющейся Overflow

}

}
```

Использование иерархий классов для обработки исключений естественным образом приводит к обработчикам, интересующимся лишь подмножеством информации, которую несут с собой исключения. Другими словами, исключение обычно перехватывается обработчиком его базового класса, а не обработчиком его собственного класса. Семантика перехвата и задания имен исключений идентична семантике функции с аргументом. Из этого следует, что сгенерированное исключение «срезается» до перехваченного. Например:

```
Class Math_err

{

// …

virtual void debug_print() const

{ cerr << “ Математическая ошибка”; }

};
```

```
Class Int_overflow : public Math_err

{

const char* op;

int a1, a2;

Public:

Int_overflow(const char* p, int a, int b)

{ op = p; a1 = a; a2 = b; }

virtual void debug_print() const

{ cerr << ‘ ’ << op << ‘(’ << a1 << ‘,’ << a2 << ‘)’; }

// …

};

Void f()

{

try

{

g();

}

catch(Math_err m)

{

// …

}

}
```

Когда вызывается обработчик Math_err, M является объектом Math_err – даже если вызов G() привел к генерации Int_overflow. Это означает, что дополнительная информация, имеющаяся в Int_overflow, недоступна.

Во избежание потери информации можно использовать указатели или ссылки. Например:

```
Int add(int x, int y)

{

if((x > 0 && y > 0 && x > INT_MAX — y)||

( x < 0 && y < 0 && x < INT_MIN — y))

throw Int_overflow(“+”, x, y);

return x + y;

}

Void f()

{

try

{

int i1 = add(1, 2);

int i2 = add(INT_MAX, -2);

int i3 = add(INT_MAX, 2); // Приехали!

}

catch(Mathe_rr& m)

{

// …

m. debug_print();

}

}
```

Последний вызов Add() приведет к исключению, которое вызовет Int_overflow::debug_print(). Если бы исключение перехватывалось по значению, а не по ссылке, была бы вызвана функция Math_err::debug_print().

Не каждая группа исключений является древообразной структурой. Довольно часто исключение принадлежит сразу двум группам. Например:

```
// ошибка, связанная с файлом в сети
Class NetFile_err : public NetWork_err, public FileSystem_err

{

// …

};
```

NetFile_err может перехватываться функциями, работающими с исключениями в сети:

```
Void f()

{

try { /* … */ }

catch(NetWork_err& nwe) { /* … */ }

}
```

А также функциями, работающими с исключениями файловой системы:

```
Void g()

{

try { /* … */ }

catch(FileSystem_err& fse) { /* … */ }

}
```

Такая иерархическая организация обработки ошибок имеет большое значение в тех случаях, когда службы (например, сетевые) прозрачны для пользователя. В этом примере автор G() мог и не подозревать о существовании сети.

Рассмотрим пример:

```
Void f()

{

try
```

```
{

throw E();

}

catch(H) { /* … */ }

}
```

Обработчик будет вызван:

1) если H того же типа, что и E;

2) если H является открытым базовым классом E;

3) если H и E являются указателями, и 1 или 2 выполняется для типов, на которые они ссылаются;

4) если H и E являются ссылками, и 1 или 2 выполняется для типа, на который H ссылается.

Кроме того, можно добавить модификатор Const к типу, используемому для перехвата исключения. Это воспрепятствует модификации перехваченного исключения.

Обработка исключений в конструкторах и деструкторах

Исключения предоставляют способ решить следующую проблему: как сообщить об ошибке из конструктора. В виду того, что конструктор не возвращает отдельного значения, которое вызывающая функция могла бы проверить, традиционными (то есть без обработки исключений) альтернативами остаются:

Возвратить объект в «неправильном» состоянии и полагаться на то, что пользователь проверит его состояние;

Присвоить значение нелокальной переменной (например, Errno) для указания на неуспешное создание объекта и полагаться на то, что пользователь проверит значение переменной;

Не осуществлять никакой инициализации в конструкторе и полагаться на то, что пользователь вызовет функцию инициализации до первого использования;

Пометить объект как неинициализированный и при первом вызове функции-элемента для этого объекта осуществить инициализацию (такая функция – не конструктор – может вернуть сообщение об ошибке в случае неуспешной инициализации).

Обработка исключений позволяет передать информацию неуспешной инициализации из конструктора. Например, простой класс Vector мог бы защититься от запроса слишком большого количества памяти следующим образом:

```
Class Vector

{

Public:

class Size_err { };

enum { max = 32000 };
```

```
Vector(int sz)

{

if(sz < 0 || sz > max) throw Size();

// …

}

}
```

Код, создающий вектора, теперь может перехватывать ошибки Vector::Size_err, которые можно каким-либо образом обработать:

```
Vector* f(int s)

{

try

{

Vector* p = new Vector(s)

// …

return p;

}

catch(Vector::Size_err)

{

// обработка ошибки размера вектора

}

}
```

Когда код, инициализирующий элемент (непосредственно или косвенно), генерирует исключение, оно (по умолчанию) передается туда, где вызван конструктор для класса этого элемента. Однако сам конструктор может перехватывать такие исключения, помещая все тело функции, включая список инициализаторов элементов, в блок Try. Например:

```
Class X

{

Vector v;

// …

Public:

X(int);

// …

};

X::X(int s)

Try : v(s) // инициализация v при помощи s

{

// …

}

Catch(Vector::Size_err) // перехват исключений

{ // сгенерированных при

// … // инициализации v

}
```

С точки зрения обработки исключений деструктор может вызываться одним из двух способов:

Нормальный вызов: в результате нормального выхода имени из области видимости, использования оператора Delete и т. д.;

Вызов в процессе обработки исключения: в процессе раскручивания стека механизм обработки исключения приводит к выходу из области видимости, содержащей объект с деструктором.

Во втором случае исключение не должно покинуть сам деструктор. Если все-таки покинет, это считается ошибкой механизма обработки исключений и вызывается Std::terminate(). Все же не существует общего способа определить, в праве ли механизм обработки исключений или деструктор проигнорировать одно исключение ради обработки другого.

Деструктор в состоянии защитить себя, если он вызывает функции, которые могут сгенерировать исключения. Например:

```
X::~X() try

{

f(); // может сгенерировать исключение

}

Catch(…)

{

// некоторые действия

}
```

Структурное управление исключениями

В современных системах программирования на языках C/C++ существует механизм так называемого структурного управления исключениями, где исключения идентифицируются только типом Unsigned int. Структурное управление исключениями позволяет наряду с обработкой потока явно порождаемых программой исключений обрабатывать и исключения, порождаемые операционной системой в аварийных ситуациях. Этим объясняется наличие единственного типа идентификации исключений и, как следствие, единственного блока обработки исключений в контролируемом блоке программы.

Различают две разновидности структурного управления исключениями:

Кадрированное управление – блок обработки исключений активизируется только в момент порождения исключения;

Завершающее управление – любой вид выхода из контролируемого блока программы завершается активизацией предопределенного блока операторов.

Операторы контролируемого блока могут явно породить исключение, используя функцию

```
VOID RaiseException (

DWORD dwExceptionCode,

DWORD dwExceptionFlags,

DWORD nNumberOfArguments,

CONST DWORD *lpArguments );
```

Интерпретация параметров функции RaiseException:

DwExceptionCode – код исключения;

DwExceptionFlags – флаг возобновления исключения;

NNumberOfArguments – количество аргументов детализации описания исключения в массиве LpArguments.

Предопределенные коды исключений:

EXCEPTION_ACCESS_VIOLATION – чтение или запись по адресу, не имея на то соответствующих прав;

EXCEPTION_DATATYPE_MISALIGNMENT – попытка чтения или записи данных с нарушением выравнивания;

EXCEPTION_BREAKPOINT – достигнута точка прерывания;

EXCEPTION_SINGLE_STEP – сигнал о том, что одиночная команда была выполнена;

EXCEPTION_ARRAY_BOUNDS_EXCEEDED – выход за пределы массива;

EXCEPTION_FLT_DENORMAL_OPERAND – недопустимое значение операнда в операциях с плавающей точкой;

EXCEPTION_FLT_DIVIDE_BY_ZERO – попытка деления на ноль в операциях с плавающей точкой;

EXCEPTION_FLT_INEXACT_RESULT – результат операции с плавающей точкой не может быть представлен в виде десятичной дроби;

EXCEPTION_FLT_INVALID_OPERATION – любое другое исключение в операциях с плавающей точкой, не включенное в этот список;

EXCEPTION_FLT_OVERFLOW – операция с плавающей запятой вызвала переполнение;

EXCEPTION_FLT_STACK_CHECK – переполнение стека в операциях с плавающей точкой

EXCEPTION_FLT_UNDERFLOW – операция с плавающей запятой вызвала антипереполнение;

EXCEPTION_INT_DIVIDE_BY_ZERO – попытка деления на ноль в операциях с целыми;

EXCEPTION_INT_OVERFLOW – результат целочисленной операции вызвал переполнение;

EXCEPTION_PRIV_INSTRUCTION – попытка выполнить команду недопустимую для текущего режима;

EXCEPTION_IN_PAGE_ERROR – попытка обращения к неизвестной странице;

EXCEPTION_ILLEGAL_INSTRUCTION – попытка выполнения недопустимой инструкции;

EXCEPTION_NONCONTINUABLE_EXCEPTION – попытка продолжить выполнение команд, после возникновения исключение не позволяющее этого;

EXCEPTION_STACK_OVERFLOW – переполнение стека;

Таким образом, предопределенные исключения достаточно подробно представляют ошибки, обнаруживаемые операционной системой.

Кадрированное управление исключениями

Синтаксис определения кадрированного управления исключениями:

```
__try

{
```

```
// Операторы контролируемого блока

}

__except(выражение_фильтра)

{

// Операторы блока обработки исключения

}
```

Блок обработки исключения можно рассматривать как условный оператор, где решение о продолжении процесса определяется вычисляемым после порождения исключения выражением фильтра.

Выражение фильтра может принимать одно из значений:

EXCEPTION_EXECUTE_HANDLER (1) – обработать исключение;

EXCEPTION_CONTINUE_SEARCH (0) – продолжение поиска обработчика исключения на предшествующем уровне вложенности оператора __try;

EXCEPTION_CONTINUE_EXECUTION (-1) – возврат управления в точку выброса исключения.

Как в выражении фильтра, так и в блоке обработки исключения можно получить детальную информацию о причине исключения, вызывая функции

DWORD GetExceptionCode(VOID);

LPEXCEPTION_POINTERS GetExceptionInformation(VOID);

Функция GetExceptionCode() возвращает код исключения, а GetExceptionInformation() – указатель на структуру EXCEPTION_POINTERS, которая представляет собой детальное описание исключения.

Завершающее управление исключениями

Синтаксис определения завершающего управления исключениями:

```
__try

{

// Операторы контролируемого блока

}

__finally

{

// Операторы блока обработки факта завершения

// контролируемого блока

}
```

Завершение контролируемого блока может быть нормальным или преждевременно прерванным. Причины досрочного выхода:

Выполнение оператора Return, Goto, Break или Continue;

Вызов функции, подобной Longjump();

Порождение исключения.

Любой исход завершения контролируемого блока, безусловно приводит к гарантированному выполнению операторов блока __finally. Очевидно, что допускается совмещение кадрированного и завершающего управления исключениями. Например:

```
Void main()

{

puts("Начало программы");

int *p = 0x00000000; // Пустой указатель!

__try

{

puts("Начало блока контроля исключения");

__try

{

puts("Начало блока контроля завершения");

puts("Попытка нарушения защиты памяти…");

*p = 13;

puts("Продолжение работы");

}

__finally

{

puts("Блок завершения активен");

}

puts("Конец блока контроля исключения");
```

```
}

__except(puts("Фильтр активен"), 1)

{

puts("Исключение обработано");

}

puts("Завершение программы");

}
```

Результаты работы программы:
Начало программы
Начало блока контроля исключения
Начало блока контроля завершения
Попытка нарушения защиты памяти…
Фильтр активен
Блок завершения активен
Исключение обработано
Завершение программы

Практическое занятие № 31-32

Тема: Разработка политики безопасности, перекрывающей каналы передачи персональных данных сотрудников и контрагентов по электронной почте.

Цель: разработать по примеру политику безопасности, перекрывающей каналы передачи персональных данных сотрудников и контрагентов по электронной почте

Теоретическая часть:

Политика обработки персональных данных: образец

В соответствии со ст. 18.1 Федерального закона № 152-ФЗ «О персональных данных» в обязанности оператора персональных данных входит издание документа, определяющего его политику в отношении защиты и обработки персональных данных.

Что это за документ? Не стоит путать его с Положением о персональных данных. Положение о персональных данных — это обязательный локальный акт, который должен быть у любого работодателя. Политика защиты и обработки персональных данных становится обязательным документом, в случае обработки персональных данных на сайте оператора. Например, когда клиенты регистрируются на сайте организации и оставляют для этого свои персональные данные.

К таким организациям, в первую очередь, относятся интернет-магазины, социальные сети и другие сайты, государственные и муниципальные органы. Это могут быть и просто организации, которые проводят конкурсы на занятие вакантных должностей и на своих сайтах выставляют имеющиеся вакансии и предлагают кандидатам заполнить анкету.

Штрафы за неправильную работу с персональными данными довольно высоки. Максимальный размер одного штрафа — 75 тыс. руб. В рамках одной проверки Роскомнадзор может обнаружить несколько разных нарушений. Тогда он взыщет сразу несколько штрафов. Чтобы избежать штрафа необходимо опубликовать на сайте

общедоступные ссылки: на Политику компании в отношении защиты и обработки персональных данных и иные сведения о требованиях к защите персональных данных.

Как составить Политику защиты и обработки персональных данных

Требования к документу, который определяет политику обработки персональных данных, содержат Рекомендации по составлению документа. Согласно рекомендациям, в Политику надо включить следующие разделы:

Общие положения

В этой части сформулируйте назначение Политики и дайте определение основных терминов, которые встречаются в документе («обработка персональных данных», «объект персональных данных», «субъект персональных данных» и т.д.), перечислите права и обязанности компании и субъектов персональных данных. Назначение политики можно сформулировать следующим образом: «защита прав субъектов персональных данных (работников, клиентов) при их обработке».

Правовые основания обработки персональных данных

Здесь дайте список нормативных актов, в соответствии с которыми вы обрабатываете персональные данные. Например:

- законы и нормативные акты, регулирующие отношения, связанные с деятельностью компании в сфере обработки персональных данных;
- учредительные документы, трудовые договоры и другие соглашения между компанией и работником;
- согласие субъекта персональных данных на их обработку.

Цели обработки персональных данных

Цель обработки персданных должна быть предметной и однозначной. Если не указать цель обработки, то сбор данных работников и клиентов будет незаконным. Отнеситесь к заполнению этого раздела максимально серьезно.

При формулировки цели опирайтесь на направления деятельности компании и анализ нормативных актов, которые регулируют эту деятельность. Лучше всего перечислить цели подробно, чтобы ничего не упустить, а не давать общие определения.

Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

Содержание и объем обрабатываемых данных должны соответствовать целям обработки.

К категориям субъектов персональных данных могут быть отнесены:

- работники оператора, бывшие работники, кандидаты на замещение вакантных должностей, родственники работников;
- клиенты и контрагенты оператора (физические лица);
- представители и работники клиентов и контрагентов оператора (юридических лиц).

В рамках каждой из категорий субъектов и применительно к конкретным целям рекомендуем перечислить все обрабатываемые оператором персональные данные, а также отдельно описать все случаи обработки специальных категорий персональных данных и биометрических персональных данных.

Порядок и условия обработки персональных данных

В этом разделе перечислите действия, которые будет совершать компания с пересданными. Укажите способы обработки, сроки обработки и хранения. Действия, совершаемые с персональными данными:

- сбор;

- запись;
- систематизация;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передача (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

При составлении текста выберите те действия, которые совершает ваша компания с данными. Обычно в Политике перечисляют все способы.

Способ обработки пересданных может быть:

- автоматизированным (с использованием средств вычислительной техники);
- неавтоматизированным (вручную).

В Политике необходимо указать способ, который используют в компании. Чаще всего указывают оба.

Срок обработки персональных данных

Срок обработки персональных данных — это период от начала обработки данных до ее прекращения. Начало обработки для каждого субъекта персональных данных будет разным. Рекомендуем разграничить начало для каждого из них. Например, срок обработки персональных данных клиентов начинается с момента регистрации на сайте или заключения договора, а срок обработки данных сотрудников — с начала действия трудового договора. Дата прекращения обработки персональных данных определяется моментом наступления одного из событий:

- достигнута цель обработки;
- истек срок действия согласия субъекта или он отозвал согласие на обработку данных;
- обнаружена несанкционированная обработка данных;
- организация прекратил свою деятельность. Сколько хранить персональные данные.

Персональные данные не стоит хранить дольше того срока, который нужен для их обработки. Лучше всего указать конкретную дату (число, месяц, год) и основание, которое станет причиной прекращения обработки персональных данных.

Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

В случае если персональные данные указаны не точно или обнаружена их несанкционированная обработка, оператор должен актуализировать информацию или прекратить обработку персональных данных. В этой связи пропишите в политике, что ваша компания обязана внести изменения, уничтожить или блокировать данные, если субъект представит вам сведения о том, что данные устарели, недостоверны или получены незаконно. Пропишите срок, в течение которого субъект должен сообщить эти сведения.

Кроме этих разделов, в Политику рекомендуется включать регламент(ы) реагирования на запросы, обращения субъектов персональных данных и их представителей, уполномоченных органов по поводу неточности персональных данных,

неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к своим данным, а также соответствующие формы запросов и обращений.

Политика утверждается приказом руководителя. Если принимается новая Политика, приказом следует отменить предыдущую и утвердить новую редакцию Политики.

С Политикой необходимо ознакомить всех работников организации под подпись. Напомним еще раз, что Политика обязательно должна быть размещена на сайте компании.

Задание: разработать по примеру политику безопасности, перекрывающей каналы передачи персональных данных сотрудников и контрагентов по электронной почте.

Практическое занятие № 33-34

Тема: Разработка политики безопасности, перекрывающей каналы передачи базы клиентов организации в архиве с использованием файловых протоколов.

Теоретическая часть:

Краткое введение

Файловые системы современных операционных систем при соответствующей настройке эффективно обеспечивают безопасность и надежность хранения данных на дисковых накопителях. Для операционных систем Windows стандартной является файловая система NTFS.

Устанавливая для пользователей определенные разрешения для файлов и каталогов (папок), администраторы могут защитить информацию от несанкционированного доступа. Каждый пользователь должен иметь определенный набор разрешений на доступ к конкретному объекту файловой системы. Кроме того, он может быть владельцем файла или папки, если сам их создает. Администратор может назначить себя владельцем любого объекта файловой системы, но обратная передача владения от администратора к пользователю невозможна.

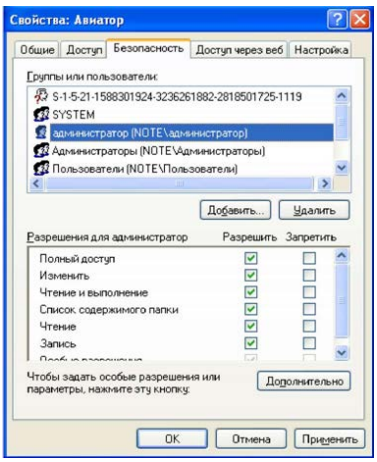
Назначение разрешений производится для пользователей или групп. Так как рекомендуется выполнять настройки безопасности для групп, то необходимо, чтобы пользователь был членом хотя бы одной группы на компьютере или в домене.

Разрешения могут быть установлены для различных объектов компьютерной системы, однако в настоящем издании рассмотрены разрешения для файлов и папок. Другие задачи, например разрешения для принтеров, решаются аналогичным образом.

Указания к проведению практического занятия

Для назначения разрешений для файла или папки администратор выбирает данный файл или папку и при нажатии правой кнопки мыши использует команду Свойства (Properties), в появившемся окне переходит на вкладку Безопасность (Security). Пример для папки с именем Авиатор приведен на рис. 4.1.

В зоне Имя (Name) имеется список групп и пользователей, которым уже назначены разрешения для данного файла или папки.



Для добавления пользователя или группы нажмите кнопку Добавить (Add) или Удалить (Remove). При добавлении появится диалог Выбор: Пользователи, Компьютеры или Группы (Select Users, Computers or Groups). Добавив пользователя или группу, мы увидим этот объект в зоне Имя и, выделив его, можем задать необходимые разрешения с помощью установки флажков Разрешить (Allow) или Запретить (Deny) в зоне Разрешения (Permissions).

Стандартные разрешения для файлов:

• полный доступ (Full Control);
• изменить (Modify);
• чтение и выполнение (Read&Execute);
• чтение (Read);
• запись (Write).

Стандартные разрешения для папок:

• полный доступ (Full Control);
• изменить (Modify);
• чтение и выполнение (Read&Execute);
• список содержимого папки;
• чтение (Read);
• запись (Write).

Разрешение Чтение позволяет просматривать файлы и папки и их атрибуты.

Разрешение Запись позволяет создавать новые файлы и папки внутри папок, изменять атрибуты и просматривать владельцев и разрешения.

Разрешение Список содержимого папки позволяет просматривать имена файлов и папок.

Разрешение Чтение и выполнение для папок позволяет перемещаться по структуре других папок и служит для того, чтобы разрешить пользователю открывать папку, даже если он не имеет прав доступа к ней, для поиска других файлов или вложенных папок. Разрешены все действия, право на которые дают разрешения Чтение и Список содержимого папки. Это же разрешение для файлов позволяет запускать файлы программ и выполнять действия, право на которые дает разрешение Чтение.

Разрешение Изменить позволяет удалять папки, файлы и выполнять все действия, право на которые дают разрешения Запись и Чтение и выполнение.

Разрешение Полный доступ позволяет изменять разрешения, менять владельца, удалять файлы и папки и выполнять все действия, на которые дают право все остальные разрешения NTFS.

Разрешения для папок распространяются на их содержимое: под- папки и файлы.

При назначении пользователю или группе разрешения на доступ к файлу или папке руководствуются тем уровнем доступа, который достаточен для данной группы или пользователя при выполнении им своих рабочих обязанностей.

Рассмотренные разрешения относятся к пользователям данного компьютера, совершившим вход локально на данную машину. Такие разрешения называются разрешениями файловой системы.

Так как файловая система Windows называется NTFS, то разрешения файловой системы для Windows называют разрешениями NTFS.

Разрешения для пользователей, получивших доступ к папке или файлу через сеть, регулируются отдельно с помощью так называемых разрешений общего доступа. Эти разрешения распространяются только на папки, к которым предоставлен общий доступ через сеть, и действуют только для пользователей, обращающихся к папке через сеть. Возможности пользователя задаются разрешениями, представленными ниже:

• полный доступ (Full Control);

• изменить (Change);

• чтение (Read).

Доступ к средствам настройки разрешений общего доступа выполняется через свойства папки, предоставленной в общий доступ (рис. 4.2).

Разрешения общего доступа - средство обеспечения безопасности данных при коллективной работе с документами. Они должны устанавливаться очень тщательно и обоснованно. При этом администратору рекомендуется действовать следующим образом.

• Для каждого ресурса общего доступа определить, каким группам пользователей необходим доступ к нему и какой требуется уровень доступа.

• Для упрощения администрирования назначать

разрешения группам, а не отдельным пользователям.

• Устанавливать максимально строгие разрешения, которые, однако, должны позволять пользователям совершать необходимые действия.

• Организовать ресурсы общего доступа таким образом, чтобы папки с одинаковым уровнем требований безопасности находились в одной папке. Затем установить общий доступ только к ней, все вложенные папки наследуют настройки безопасности.

• Для папок общего доступа применять интуитивно понятные пользователям имена, корректно отображаемые всеми клиентскими операционными системами, используемыми на предприятии.

• Если в общих папках предполагается хранить программы- приложения, то целесообразно поместить их в одну папку - единое место хранения и обновления приложений.

Несколько общих папок, доступных членам группы Администраторы, так называемые скрытые административные общие папки, создается операционной системой автоматически. Имена этих папок заканчиваются знаком $. Это корневые каталоги каждого тома на жестком диске (C$, D$ и т.д.), папка Admin$ - для доступа к системному каталогу, папка Print$ - для доступа к файлам драйверов принтеров.

Кроме того, скрытую папку с общим доступом можно создать с целью доступа к ней только тех пользователей, которые будут знать имя скрытой папки.

Получить доступ к общим папкам других компьютеров можно, используя компоненты Сетевое окружение, Мой компьютер, Мастер добавления в сетевое окружение и команду Выполнить (Run).

Соединение с общей папкой через Сетевое окружение выполняется двойным щелчком по ресурсу, к которому необходимо получить доступ. Если общий ресурс

отсутствует в списке доступных, выберите значок Добавить новый элемент в сетевое окружение и укажите адрес подключаемого ресурса.

Соединение с общей папкой через компонент Мой компьютер выполняется через меню Сервис этого компонента в пункте Подключить сетевой диск посредством указания пути к общему ресурсу. Если необходимо пользоваться этим соединением постоянно, нужно, чтобы флажок Восстанавливать при входе в систему был установлен. Соединение будет доступно в разделе Сетевые диски окна Мой компьютер.

Для соединения с общей папкой с помощью команды Выполнить щелкните Пуск, затем Выполнить и введите путь к папке в формате UNC (имя_ компьютераимя_общей папки).

Рассмотрим, как пользоваться средствами установки разрешений файловой системы и общего доступа.

После выбора объекта, для которого будет выполняться настройка разрешений файловой системы, в диалоговом окне свойств файла или папки необходимо выбрать вкладку Безопасность

В данном случае видим, что для папки Авиатор для группы Администраторы установлены разрешения уровня Полный доступ, а для группы Все разрешения ограничены уровнем Чтение.

При установке разрешений в списке групп можно заметить имена так называемых встроенных системных групп, невидимых при использовании оснасток для управления группами и пользователями. Эти группы не имеют определенных членств, которые можно назначить или изменить, но в них система включает различных пользователей в различное время в зависимости от того, каким образом пользователь получает доступ к системе или ресурсам.

Встроенные системные группы были рассмотрены в практическому занятию № 3. В данном случае имеется в виду группа Все, в которую во время работы входят все, кто получил доступ к компьютеру или домену.

Разрешения можно не только устанавливать, но и запрещать. Запрет имеет больший приоритет, чем разрешение. Запрет разрешений как метод контроля ресурсов применять не рекомендуется, и он используется в основном для дополнительной настройки разрешений конкретным пользователям в отличие от разрешений для остальных пользователей группы.

Рассмотренные разрешения называются стандартными и позволяют решить большинство задач, связанных с регулированием уровня доступа групп к ресурсам.

Кнопка Дополнительно (см. рис. 4.3) служит для задания специальных разрешений. Каждое стандартное разрешение состоит из нескольких специальных. Например, стандартное разрешение Запись включает в себя шесть специальных разрешений: создание файлов/запись данных, создание папок/дозапись данных, запись атрибутов, запись дополнительных атрибутов, чтение разрешений, синхронизация. Специальные разрешения можно использовать для настройки в нестандартных ситуациях.

В окне специальных разрешений имеются закладки Аудит, Владелец и Эффективные разрешения.

Аудит - это процесс, позволяющий фиксировать события, происходящие в системе и имеющие отношение к безопасности. На данной вкладке производится выбор пользователя или группы, для которых данная папка (или файл) будет объектом аудита. Аудит изучается в практическому занятию № 5.

Закладка Владелец обеспечивает такое свойство безопасности, как право владения объектом файловой системы. Администратор всегда может стать владельцем любого объекта файловой системы, любой пользователь - владелец созданных им объектов. Если локальные или доменные политики безопасности разрешат, пользователь может назначать себя владельцем других файлов и папок.

Подробное рассмотрение вопросов владения выходит за рамки данного издания, однако отметим, что многие операции с файлами и папками, например смена разрешений, шифрование и дешифрование, привязаны к факту владения данным объектом.

Список управления доступом (ACL) хранится на диске NTFS для каждого файла или папки. В нем перечислены пользователи и группы, для которых установлены разрешения для файла или папки, а также сами назначенные разрешения.

Каждому пользователю или группе могут быть установлены множественные разрешения через участие в нескольких группах с разным набором разрешений. В этом случае действуют эффективные разрешения - пользователь обладает всеми назначенными ему разрешениями.

Действует приоритет разрешений для файлов над разрешениями для папок и приоритет запрещения над разрешением.

Разрешения, назначенные родительской папке, по умолчанию наследуются всеми подпапками и файлами, содержащимися в папках. Однако есть возможность предотвратить наследование для любой вложенной папки. В этом случае эта папка сама становится родительской для вложенных в нее папок.

Если папка предоставлена для общего доступа, то на нее распространяются разрешения двух видов:

• разрешения файловой системы, установленные для пользователей данного компьютера;

• разрешения общего доступа, объявленные для пользователей, получивших доступ через сеть

Обычно для папок общего доступа задают разрешения полного доступа, а ограничения вводят установкой разрешений NTFS [4, 5].

В этом случае действует объединение разрешений NTFS и разрешений для общей папки, при котором наиболее строгое разрешение имеет приоритет над другими.

Задание к проведению практического занятия

1. Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe, например одну из стандартных программ Windows, такую как notepad.exe (Блокнот).

2. Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью.

3. Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.

4. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.

5. Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.

6. Экспериментально убедитесь в выполнении правил объединения разрешений NTFS и разрешений общего доступа.

7. Составьте отчет о проведенных экспериментах.

8. Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Контрольные вопросы

1. Какое из следующих разрешений NTFS для папок позволяет удалять папку:

• чтение;

• чтение и выполнение;

• изменение;

• администрирование?

2. Какое разрешение NTFS для файлов следует установить, если вы позволяете пользователям удалять файл, но не позволяете становиться его владельцами?

3. Какие объекты по умолчанию наследуют разрешения, установленные для родительской папки?

4. Кто может устанавливать разрешения для отдельных пользователей и групп (выберите все правильные ответы):

• члены группы Администраторы;

• члены группы Опытные пользователи;

• пользователи, обладающие разрешением Полный доступ;

• владельцы файлов и папок?

5. Какой из следующих вкладок диалогового окна свойств файла или папки следует воспользоваться для установки или изменения разрешений NTFS:

• Дополнительно;

• Разрешения;

• Безопасность;

• Общие

6. Если вы хотите, чтобы пользователь или группа не имели доступа к определенной папке или файлу, следует ли запретить разрешения для этой папки или файла?

Практическое занятие № 35-40

Тема: Разработка политики безопасности, перекрывающей каналы передачи информации, составляющей коммерческую тайну.

Практическая часть 1:

Правовая защита информационных ресурсов ограниченного доступа. (описать одну тайну)

Цель: научиться определять перечня видов тайн, обрабатываемых в организации

Составление перечня видов тайн, обрабатываемых в организации

Теоретический материал

Согласно ФЗ №149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и защите информации», вся информация делится на:

- информацию ограниченного доступа;

- общедоступную информацию.

УП №188 от 06 марта 1997 года «Об утверждении перечня сведений конфиденциального характера» определяет следующие виды тайн:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях. (ФЗ №152-ФЗ «О персональных данных»).

2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" и другими нормативными правовыми актами Российской Федерации. (в ред. Указа Президента РФ от 23.09.2005 N 1111).

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (профессиональная тайна: врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна ФЗ №98-ФЗ).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.(интеллектуальная собственность, ГК РФ).

Виды тайн	**Закон**	**Содержание**
Государственная тайна	- Закон №5485-1 «О государственной тайне»	Информация распространение которой может нанести ущерб РФ
Коммерческая тайна	- ФЗ №98-ФЗ «О коммерческой тайне»	Научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющаясекреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступана законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны
Служебная тайна	- УП от 6.03.1997 №188; - 139 ГК РФ; - ФЗ "Об основах государственной службы Российской Федерации"; - ПП РФ от 3.11.94г. № 1233	Служебные сведения, доступ к которым ограничен органами государственной власти всоответствии с Гражданским кодексом Российской Федерации и федеральными законами
Профессиональная тайна: - тайна связи;	УП от 6.03.1997 №188; 176-ФЗ "О почтовой связи", 126-ФЗ "О	 Тайна переписки, телефонных переговоров, почтовых, телеграфных или

	связи", УПК РФ;	иных сообщений
- медицинская тайна	223-ФЗ «Семейный кодекс РФ»	Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе заболевания, иные сведения, полученные при обследовании и лечении гражданина, а также сведения о проведенных искусственном оплодотворении и имплантации эмбриона, а также о личности донора
Персональные данные	ФЗ №152-ФЗ «О персональных данных»	Любая информация позволяющая идентифицировать личность

В зависимости от рода деятельности на предприятии может одновременно обрабатываться информация, относящаяся к разным видам информации ограниченного доступа.

Форма собственности	**Виды тайн**
Государственная	ГТ, СТ, ПрТ, ПДн
Муниципальная	СТ, ПрТ, ПДн
Коммерческая	КТ, ПрТ, ПДн
Индивидуальная	КТ, ПрТ, ПДн

Контрольные вопросы:

1. ФЗ определяющий ограничения на доступ к информации?
2. В каком документе перечислены виды тайн РФ?
3. Закон определяющий ГТ?

Практическая часть 2:

Как составить положение о коммерческой тайне

1. Перечень сведений, составляющих коммерческую тайну организации

Закон лишь дает понятие информации, составляющей коммерческую тайну, но не указывает, какие именно сведения к ней относятся. Этот перечень должны установить вы сами (п. 1 ч. 1 ст. 10 Закона о коммерческой тайне). Обычно это делают в положении о коммерческой тайне, причем перечень сведений может быть открытым.

Чтобы составить перечень информации, составляющей коммерческую тайну организации, достаточно перечислить лишь наиболее важные для вас виды информации и указать, что режим коммерческой тайны можно распространить и на другие сведения приказом руководителя организации (если это не запрещено законом).

Например, вы можете установить режим коммерческой тайны:

1) для договоров с контрагентами и информации о ходе их исполнения;

2) системы ценообразования на ваши товары, работы, услуги;

3) клиентской базы с данными текущих, бывших, потенциальных клиентов;

4) логинов и паролей для доступа к информации, хранящейся в электронном виде.

Рекомендуем убедиться, что указанная вами информация не входит в перечень сведений, которые не могут составлять коммерческую тайну.

Пример условия с перечнем сведений, составляющих коммерческую тайну

3.1. Режим коммерческой тайны устанавливается для следующей информации:

• сведения о контрагентах - покупателях товаров общества, договоры с ними и сведения о ходе исполнения договоров;

• документы, поступившие от контрагентов - покупателей товаров общества;

• принцип определения цены товара (в том числе система скидок), порядка оплаты (в том числе возможности рассрочки, отсрочки, сроков оплаты) для конкретного покупателя;

• объем товарооборота с контрагентами общества;

• информация о переговорах с потенциальными покупателями товаров общества;

• сведения о взаимодействии структурных подразделений в обществе.

3.2. Генеральный директор общества вправе своим приказом распространять режим коммерческой тайны на иную информацию, если это не запрещено законом.

Обратите внимание: вы должны проставить гриф о коммерческой тайне на материальные носители с ней или включить его в реквизиты документов, содержащих такую информацию (п. 5 ч. 1 ст. 10 Закона о коммерческой тайне). Порядок использования грифа также лучше указать в положении.

Что такое гриф "коммерческая тайна", как он выглядит и кто его ставит

Гриф о коммерческой тайне - это отметка, которая наносится на материальные носители, документы, содержащие секретную информацию. Например, у организации может быть специальный штамп для этих целей. Также гриф может входить в состав реквизитов документов, содержащих коммерческую тайну, то есть его можно напечатать как обычный текст или сделать частью фирменного бланка. Главное, чтобы он был заметен для лиц, использующих документ.

Содержание грифа определено законом. Так, если обладателем информации является юридическое лицо, гриф должен содержать полное наименование и место нахождения организации, а также слова "Коммерческая тайна" (п. 5 ч. 1 ст. 10 Закона о коммерческой тайне). По желанию можно включить в него дополнительные сведения, в частности срок действия режима коммерческой тайны или напоминание о необходимости не нарушать его, например фразу "строго конфиденциально".

Наносит гриф обычно лицо, уполномоченное на это положением о коммерческой тайне или приказом руководителя организации.

Если вы не нанесете гриф "коммерческая тайна" на носитель информации, вам будет сложнее привлечь лицо к ответственности за ее разглашение, поскольку гриф напрямую доказывает осведомленность лица в том, что оно имеет дело с секретными сведениями.

2. Доступ к информации, составляющей коммерческую тайну

Закон обязывает вас вести учет лиц, получивших доступ к информации, составляющей коммерческую тайну (п. 3 ч. 1 ст. 10 Закона о коммерческой тайне). В связи с этим рекомендуем указать в положении:

1) кто имеет доступ к информации. Удобнее указывать не имена конкретных работников, а должности, чтобы не пришлось менять положение в случае их увольнения.

Объем доступной информации может быть различным. Например, генеральный директор и главный бухгалтер, скорее всего, будут иметь доступ ко всей информации. Другим сотрудникам могут быть необходимы для работы только определенные сведения. Например, юрисконсульт должен иметь доступ к договорам, но ему вряд ли понадобится информация о ценообразовании.

Важно помнить: если работа с коммерческой тайной не предусмотрена трудовыми обязанностями работника, но тем не менее понадобилась ему, нужно получить его согласие на доступ к ней (ч. 2 ст. 11 Закона о коммерческой тайне);

2) как предоставляется и отменяется доступ к информации, составляющей коммерческую тайну. Например, для лиц, которые в силу своих трудовых обязанностей не

работают с ней на постоянной основе, порядок получения доступа может включать следующие этапы:

• руководитель подразделения направляет генеральному директору заявку, в которой обосновывает необходимость предоставить лицу доступ к секретной информации с указанием необходимого периода доступа;

• после одобрения заявки лицо знакомится с положением о коммерческой тайне и подписывает соглашение о конфиденциальности, выражая этим свое согласие на работу с секретными сведениями;

• руководитель подразделения предоставляет информацию и контролирует ее использование.

3. Сохранность сведений, составляющих коммерческую тайну

Установите, как должны храниться различные носители, на которых содержится секретная информация. Например, бумажные документы должны находиться в отдельных помещениях (шкафах, сейфах и т.д.), доступ к которым имеют только определенные лица. Документы в электронной форме целесообразно защитить паролями, которые будут знать также только допущенные к этой информации лица.

Также рекомендуем назначить ответственных лиц - сотрудников, которые будет контролировать сохранность тех или иных сведений. Как правило, ими становятся руководители подразделений. Например, коммерческий директор может контролировать сохранность информации о ценообразовании, а руководитель отдела сбыта - о клиентской базе.

Для эффективного контроля рекомендуем закрепить в положении обязанность вести журнал учета, куда следует записывать все созданные и полученные вами документы, на которые распространяется режим коммерческой тайны.

Чтобы вовремя выявлять нарушения режима коммерческой тайны и недостатки в системе ее охраны, следует проводить плановые (например, раз в год) и внеплановые проверки того, как соблюдается данное положение. Их порядок и периодичность можно также установить в положении о коммерческой тайне.

4. Использование информации, составляющей коммерческую тайну

Укажите в положении о коммерческой тайне конкретные обязанности и запреты при использовании секретной информации.

Например, можно установить обязанность лиц:

• не сообщать пароли от файлов третьим лицам;

• немедленно информировать непосредственного руководителя об утрате носителей со сведениями, составляющими коммерческую тайну;

• при прекращении трудового или иного договора передать непосредственному руководителю все материальные носители, содержащие секретную информацию.

Также в положение можно включить запреты:

• использовать информацию, составляющую коммерческую тайну, в личных целях;

• копировать ее любым способом;

• использовать при работе с ней посторонние программы, адреса электронной почты, внешние съемные устройства;

• забирать из служебных помещений носители с информацией, составляющей коммерческую тайну.

5. Передача и предоставление информации, составляющей коммерческую тайну

Вы обязаны вести учет лиц, которым предоставили или передали информацию, составляющую коммерческую тайну (п. 3 ч. 1 ст. 10 Закона о коммерческой тайне). В связи с этим необходимо установить, что передача информации третьим лицам и ее предоставление государственным и муниципальным органам возможны только с письменного согласия руководителя организации и/или ее подразделения. Факт передачи или предоставления информации целесообразно фиксировать в специальном журнале учета.

Обратите внимание, что на документах, предоставляемых государственным органам или органам местного самоуправления, обязательно должен быть нанесен гриф "Коммерческая тайна" (ч. 4 ст. 6 Закона о коммерческой тайне). Без него будет сложно доказать, что переданные документы содержали коммерческую тайну.

6. Срок действия режима коммерческой тайны

Закон не предусматривает конкретный срок действия режима коммерческой тайны и не обязывает устанавливать его в положении о коммерческой тайне. Если вы не установите срок, работник будет обязан хранить секретность сведений бессрочно, в том числе и после прекращения действия трудового договора. Такой вывод следует из п. 2 ч. 3 ст. 11 Закона о коммерческой тайне.

Если какие-то сведения с течением времени теряют свою актуальность, вы можете установить срок действия режима коммерческой тайны только в отношении них.

Если срок действия режима еще не истек, но скрывать информацию больше нет необходимости, можно досрочно отменить режим коммерческой тайны решением руководителя. Тогда нужно будет исключить соответствующий вид информации из положения о коммерческой тайне и письменно уведомить допущенных к этой информации лиц об отмене режима. На документах и носителях, где стоял гриф "коммерческая тайна" можно поставить штамп или сделать запись "погашено". Тогда использующие их лица смогут увидеть, что информация, которая ранее была секретной, более таковой не является.

Задание: составить положение о коммерческой тайне.

Практическая часть 3:

Подготовиться к семинарским занятиям по следующим темам:

1. Классификация коммерческой тайны
2. Обзор и анализ нормативно-правовых документов, регламентирующих защиту коммерческой тайны
3. Типизация АС обработки коммерческой тайны
4. Конфигурация автоматизированной системы обработки коммерческой тайны
5. Алгоритм разработки системы защиты АС обработки коммерческой тайны
6. Матрица модели нарушителя
7. Матрица модели угроз АС обработки коммерческой тайны
8. Матрица мероприятий АС
9. Разработанные организационно-распорядительные и нормативные документы

Практическая часть 4:

Теоретический материал

Аутентификация (Authentication) - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в

систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Пароль - это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе ОРГАНИЗАЦИИ (АС ОРГАНИЗАЦИИ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС ОРГАНИЗАЦИИ и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на сотрудников службы обеспечения безопасности информации (СОБИ) - администраторов средств защиты, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников СОБИ. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников СОБИ, а также ответственных за информационную безопасность в подразделениях с паролями других сотрудников подразделений ОРГАНИЗАЦИИ (исполнителей).

4. При наличии в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать уполномоченного представителя службы обеспечения безопасности информации (СОБИ).

5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри территориального органа ОРГАНИЗАЦИИ и т.п.) должна производиться уполномоченными сотрудниками СОБИ – администраторами соответствующих средств защиты немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри территориального органа ОРГАНИЗАЦИИ и другие обстоятельства) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

8. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.6 или п.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или руководителя подразделения в опечатанном личной печатью пенале (возможно вместе с персональными ключевыми дискетами и идентификатором Touch Memory).

10. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в подразделениях (руководителей подразделений), периодический контроль – возлагается на сотрудников СОБИ – администраторов средств парольной защиты.

Контрольные вопросы:

1. Перечислить виды паролей

2. От чего зависит надежность пароля?
3. Что такое парольная политика?

Практическая часть 5:

Краткие теоретические сведения

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене, так и по своим функциональным возможностям. Наиболее мощные (и как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании обеспечить разностороннюю защиту компьютерной системы.

Большинство современных антивирусных пакетов выполняют следующие функции:

- сканирование памяти и содержимого дисков;
- сканирование в реальном режиме времени с помощью резидентного модуля;
- распознавание поведения, характерного для компьютерных вирусов;
- блокировка и/или удаление выявленных вирусов;
- восстановление зараженных информационных объектов;
- принудительная проверка подключенных к корпоративной сети компьютеров;
- удаленное обновление антивирусного программного обеспечения и баз данных через Интернет;
- фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;
- выявление потенциально опасных Java-апплетов и модулей ActiveX;
- ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты и др.

Задание

Подготовить краткий доклад по заданному вопросу (см. вариант), используя любые доступные источники информации.

Рекомендация: Собранный материал будет наиболее актуальным, если включить в него данные, полученные практическим путем. Для этого при возможности, установите демонстрационную версию заданного пакета ПО и протестируйте ее в течении нескольких дней.

1. Заполнить таблицу " Пакеты антивирусных программ " на основе подготовленного материала, а также докладов других студентов.
2. Провести анализ собранной информации и сделать выводы.

Практическая часть 6:

1. Краткие теоретические сведения

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов **– Концепции и Политики информационной безопасности.** Если Концепция ИБ в общих чертах определяет, **ЧТО** необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит **КАК**, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;

- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности**.**

3. Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.

- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия .
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

Практическое занятие № 41-42

Тема: Занесение политики информационной безопасности в DLP- систему

Практическая часть:

1. Запустить консоль «Локальные политика безопасности», перейти к настройке «Политике учётных записей».
2. Перейти к пункту «Пороговое значение блокировки» в «Политике блокировки учётной записи», установить параметр равный 3 попыткам.
3. Перейти к пункту «Минимальная длина пароля» в «Политике паролей», установить значение 10.
4. Перейти к пункту «Пароль должен отвечать требованиям сложности», поставить галочку.

Длина пароля может достигать 128 знаков. Маленький отрывок из поэмы А.С.Пушкина «Руслан и Людмила» со всеми знаками препинания, набранный русскими буквами в латинской раскладке и установленный в качестве пароля, может привести в замешательство любого взломщика: E kerjvjhmz le, ptktysq, Pkfnfz wtgm yf le,t njv, B lytv b yjxm. Rjn extysq, Dct [jlbn gj wtgb rheujv/. Этот пароль надежный, а запомнить его очень просто: «У лукоморья дуб зеленый, златая цепь на дубе том, и днём и ночью кот учёный, всё ходит по цепи кругом».

Кроме того, специалистами были разработаны рекомендации по созданию усиленных паролей, использование которых уменьшает вероятность успешной атаки взломщика:

- пароль должен содержать не менее 6 символов, и среди них должны быть символы по крайней мере трех типов из следующих четырех: заглавные буквы, строчные буквы, цифры и специальные символы (то есть ,%,*,&,!)
- пароль не может включать учётное имя пользователя;
- если пользователь создаёт пароль, который не отвечает перечисленным требованиям, операционная система выдает сообщение об ошибке и не принимает пароль.

5. Проверить действие установленных настроек.

Политика аудита

В процессе аудита используются три средства управления: политика аудита, параметры аудита в объектах, а также журнал **«Безопасность»**, куда заносятся события, связанные с безопасностью, такие как вход/выход из системы, использование привилегий и обращение к ресурсам.

Политика аудита настраивает в системе определённого пользователя и группы аудит активности. Для того чтобы отконфигурировать политики аудита, в редакторе управления групповыми политиками необходимо открыть узел **«Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Локальные политики /Политика аудита»**. Необходимо помнить, что по умолчанию параметр

политики аудита, для рабочих станций установлен на **«Не определено»**. В общей сложности, возможна настройка девяти политик аудита.

Так же, как и с остальными политиками безопасности, для настройки аудита нужно определить параметр политики. После двойного нажатия левой кнопкой мыши на любом из параметров, установите флажок на опции **«Определить следующие параметры политики»** и укажите параметры ведения аудита успеха, отказа или обоих типов событий.

После настройки политики аудита события будут заноситься в журнал безопасности. Просмотреть эти события можно в журнале безопасности.

Аудит входа в систему. Текущая политика определяет, будет ли операционная система пользователя, для компьютера которого применяется данная политика аудита, выполнять аудит каждой попытки входа пользователя в систему или выхода из неё. Например, при удачном входе пользователя на компьютер генерируется событие входа учётной записи. События выхода из системы создаются каждый раз, когда завершается сеанс вошедшей в систему учётной записи пользователя. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Аудит доступа к объектам. Данная политика безопасности выполняет аудит попыток доступа пользователей к объектам, которые не имеют отношения к Active Directory. К таким объектам можно отнести файлы, папки, принтеры, разделы системного реестра, которые задаются собственными списками в системном списке управления доступом (SACL). Аудит создаётся только для объектов, для которых указаны списки управления доступом, при условии, что запрашиваемый тип доступа и учётная запись, выполняющая запрос, соответствуют параметрам в данных списках.

Аудит доступа к службе каталогов. При помощи этой политики безопасности можно определить, будет ли выполняться аудит событий, указанных в системном списке контроля доступа (SACL), который можно редактировать в диалоговом окне **«Дополнительные параметры безопасности»** свойств объекта Active Directory. Аудит создаётся только для объектов, для которых указан системный список управления доступом, при условии, что запрашиваемый тип доступа и учётная запись, выполняющая запрос, соответствуют параметрам в данном списке. Данная политика в какой-то степени похожа на политику **«Аудит доступа к объектам»**. Аудит успехов означает создание записи аудита при каждом успешном доступе пользователя к объекту Active Directory, для которого определена таблица SACL. Аудит отказов означает создание записи аудита при каждой неудачной попытке доступа пользователя к объекту Active Directory, для которого определена таблица SACL.

Аудит изменения политики. Эта политика аудита указывает, будет ли операционная система выполнять аудит каждой попытки изменения политики назначения прав пользователям, аудита, учётной записи или доверия. Аудит успехов означает создание записи аудита при каждом успешном изменении политик назначения прав пользователей, политик аудита или политик доверительных отношений. Аудит отказов означает создание записи аудита при каждой неудачной попытке изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Аудит изменения привилегий. Используя эту политику безопасности, можно определить, будет ли выполняться аудит использования привилегий и прав пользователей. Аудит успехов означает создание записи аудита для каждого успешного применения права пользователя. Аудит отказов означает создание записи аудита для каждого неудачного применения права пользователя.

Аудит отслеживания процессов. Текущая политика аудита определяет, будет ли операционная система выполнять аудит событий, связанных с процессами, такими как создание и завершение процессов, а также активация программ и непрямой доступ к объектам. Аудит успехов означает создание записи аудита для каждого успешного события, связанного с отслеживаемым процессом. Аудит отказов означает создание записи аудита для каждого неудачного события, связанного с отслеживаемым процессом.

Аудит системных событий. Данная политика безопасности имеет особую ценность, так как именно при помощи этой политики можно узнать, перегружался ли у пользователя компьютер, превысил ли размер журнала безопасности пороговое значение предупреждений, была ли потеря отслеженных событий из-за сбоя системы аудита и даже вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени. Аудит успехов означает создание записи аудита для каждого успешного системного события. Аудит отказов означает создание записи аудита для каждого неудачного завершения системного события.

Аудит событий входа в систему. При помощи этой политики аудита можно указать, будет ли операционная система выполнять аудит каждый раз при проверке данным компьютером учётных данных. При использовании этой политики создаётся событие для локального и удаленного входа пользователя в систему. Члены домена и компьютеры, не входящие в домен, являются доверенными для своих локальных учётных записей. Когда пользователь пытается подключиться к общей папке на сервере, в журнал безопасности записывается событие удалённого входа (события выхода из системы не записываются). Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Аудит управления учётными записями. Эта последняя политика тоже считается очень важной, так как именно при помощи неё можно определить, необходимо ли выполнять аудит каждого события управления учётными записями на компьютере. В журнал безопасности будут записываться такие действия как создание, перемещение и отключение учётных записей, а также изменение паролей и групп. Аудит успехов означает создание записи аудита для каждого успешного события управления учётными записями. Аудит отказов означает создание записи аудита для каждого неудачного события управления учётными записями

Политики назначения прав пользователей

Как говорилось выше, для назначения прав пользователей существует 44 политики безопасности. Далее можно ознакомиться с восемнадцатью политиками безопасности, которые отвечают за назначение различных прав для пользователей или групп вашей организации.

1. **Архивация файлов и каталогов**. При помощи данной политики можно указать пользователей или группы, предназначенные для выполнения операций резервного копирования файлов, каталогов, разделов реестра и других объектов, которые подлежат архивации. Данная политика предоставляет доступ для следующих разрешений:

- обзор папок/выполнение файлов;
- содержимое папки/чтение данных;
- чтение атрибутов;
- чтение расширенных атрибутов;
- чтение разрешений.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**, а на контроллерах домена – **«Операторы архивации»** и **«Операторы сервера»**.

2. **Блокировка страниц в памяти**. Используя эту политику безопасности, можно указать конкретных пользователей или группы, которым разрешается использовать процессы для сохранения данных в физической памяти для предотвращения сброса данных в виртуальную память на диске.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

3. **Восстановление файлов и каталогов**. Эта политика позволяет указывать пользователей и группы, которые могут выполнять восстановление файлов и каталогов, в обход блокировке файлов, каталогов, разделов реестра и прочих объектов, расположенных в архивных версиях файлов.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**, а на контроллерах домена – **«Операторы архивации»** и **«Операторы сервера»**.

4. **Вход в качестве пакетного задания**. При создании задания, используя планировщик заданий, операционная система регистрирует пользователя в системе как пользователя с пакетным входом. Данная политика разрешает группе или определённому пользователю входить в систему при помощи такого метода.

По умолчанию, как на рабочих станциях, так и на контроллерах домена, данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**.

5. **Вход в качестве службы**. Некоторые системные службы осуществляют вход в операционную систему под разными учётными записями. Например, служба **«Windows Audio»** запускается под учётной записью **«Локальная служба»**, служба **«Телефония»** использует учётную запись **«Сетевая служба»**. Данная политика безопасности определяет, какие учётные записи служб могут зарегистрировать процесс в качестве службы.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

6. **Выполнение задач по обслуживанию томов**. Используя эту политику, можно указать пользователей или группы, участники которых могут выполнять операции, предназначенные для обслуживания томов. У пользователей, обладающих такими привилегиями, есть права на чтение и изменение запрошенных данных после открытия дополнительных файлов, они также могут просматривать диски и добавлять файлы в память, занятую другими данными.

По умолчанию, такими правами обладают только администраторы рабочих станций и контроллеров домена.

7. **Добавление рабочих станций к домену**. Эта политика отвечает за разрешение пользователям или группам добавлять компьютеры в домен Active Directory. Пользователь, обладающий данными привилегиями, может добавить в домен до десяти компьютеров.

По умолчанию, все пользователи, прошедшие проверку подлинности, на контроллерах домена могут добавлять до десяти компьютеров.

8. **Доступ к диспетчеру учётных данных от имени доверенного вызывающего**. Диспетчер учётных данных – это компонент, который предназначен для хранения учётных данных, таких как имена пользователей и пароли, используемых для входа на веб-сайты или другие компьютеры в сети. Эта политика используется

диспетчером учётных данных в ходе архивации и восстановления, и её не желательно предоставлять пользователям.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

9. **Доступ к компьютеру из сети**. Данная политика безопасности отвечает за разрешение подключения к компьютеру по сети указанным пользователям или группам.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**, **«Пользователи»** и **«Все»**. На контроллерах домена – **«Администраторы»**, **«Проверенные пользователи»**, **«Контроллеры домена предприятия»** и **«Все»**.

10. **Завершение работы системы**. Используя этот параметр политики, можно составить список пользователей, которые имеют право на использование команды **«Завершение работы»** после удачного входа в систему.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»**, **«Операторы архивации»** и **«Пользователи»** (только на рабочих станциях), а на контроллерах домена – **«Администраторы»**, **«Операторы архивации»**, **«Операторы сервера»** и **«Операторы печати»**.

11. **Загрузка и выгрузка драйверов устройств**. При помощи текущей политики можно указать пользователей, которым будут предоставлены права на динамическую загрузку и выгрузку драйверов устройств в режиме ядра.

Эта политика не распространяется на PnP-устройства. **Plug and Play** – технология, предназначенная для быстрого определения и конфигурирования устройств в компьютере и других технических устройствах. Разработана фирмой Microsoft при содействии других компаний. Технология PnP основана на использовании объектно-ориентированной архитектуры, ее объектами являются внешние устройства и программы. Операционная система автоматически распознает объекты и вносит изменения в конфигурацию абонентской системы.).

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»**, а на контроллерах домена – **«Администраторы»** и **«Операторы печати»**.

12. **Замена маркера уровня процесса**. Используя данную политику безопасности, можно ограничить пользователей или группу от использования API-функции CreateProcessAsUser для того, чтобы одна служба могла запускать другую функцию, процесс или службу. Стоит обратить внимание на то, что такое приложение как **«Планировщик заданий»** для своей работы использует данные привилегии.

По умолчанию, как на рабочих станциях, так и на контроллерах домена, данные привилегии предоставляются учётным записям **«Сетевая служба»** и **«Локальная служба»**.

13. **Запретить вход в систему через службу удалённых рабочих столов**. При помощи данной политики безопасности можно ограничить пользователей или группы от входа в систему в качестве клиента удалённых рабочих столов.

По умолчанию, как на рабочих станциях, так и на серверах, всем разрешено входить в систему как клиенту удалённых рабочих столов.

14. **Запретить локальный вход**. Данная политика запрещает отдельным пользователям или группам выполнять вход в систему.

По умолчанию всем пользователям разрешен вход в систему.

15. **Изменение метки объектов**. Благодаря данной политике назначения прав, можно предоставить возможность указанным пользователям или группам изменять метки целостности объектов других пользователей, таких как файлы, разделы реестра или процессы.

    По умолчанию никому не разрешено изменять метки объектов.

16. **Изменение параметров среды изготовителя**. Используя эту политику безопасности, можно указать пользователей или группы, которым будет доступна возможность чтения переменных аппаратной среды. Переменные аппаратной среды – это параметры, сохраняемые в энергонезависимой памяти компьютеров, архитектура которых отлична от x86.

На рабочих станциях и контроллерах домена, по умолчанию данные привилегии предоставляются группам **«Администраторы»**.

17. **Изменение системного времени**. Эта политика отвечает за изменение системного времени. Предоставив данное право пользователям или группам, тем самым кроме разрешения изменения даты и времени внутренних часов предоставляется возможность изменения соответствующего времени отслеживаемых событий в оснастке **«Просмотр событий»**.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Локальная служба»**, а на контроллерах домена – **«Администраторы»**, **«Операторы сервера»** и **«Локальная служба»**.

18. **Изменение часового пояса**. При помощи текущей политики безопасности, можно указать пользователей или группы, которым разрешено изменять часовой пояс своего компьютера для отображения местного времени, которое представляет собой сумму системного времени компьютера и смещения часового пояса.

На рабочих станциях и контроллерах домена по умолчанию данные привилегии предоставляются группам **«Администраторы»** и **«Пользователи»**.

Параметры безопасности

Узел «Параметры безопасности» позволяет администратору безопасности вручную настраивать уровни безопасности, назначенные политике локального компьютера. Чтобы изменить любое из значений шаблона, необходимо дважды щёлкнуть его. Появится диалоговое окно, позволяющее модифицировать значение.

Таким образом контролировать включение или отключение настроек безопасности, таких как цифровая подпись данных, имена учётных записей администратора и гостя, доступ к дисководам гибких и компакт-дисков, установка драйверов и приглашения на вход в систему и все остальные доступные параметры политики безопасности. Далее будут рассмотрены подробнее, какие параметры рекомендуется устанавливать для повышения защиты компьютера от различного рода атак по сети Интернет.

Первое – напоминать пользователям об истечении срока действия пароля – 14 дней (по умолчанию).

Рекомендуется включать политику «Не отображать последнего имени пользователя в диалоге входа» (по умолчанию – отключен). Особенно полезно в случае, когда рядовой пользователь имеет пароль аналогичный своему имени, и тогда без труда можно с нескольких переборов пароля хакеру проникнуть на этот компьютер.

Рекомендуется включать политику «Запретить пользователям установку драйвера принтера» (по умолчанию – отключен). А также рекомендуется включить политику «Очистка страничного файла виртуальной памяти» (по умолчанию – отключен). После

этого система всегда при выключении компьютера будет удалять файл подкачки. Но здесь есть свой недостаток – система будет долго выключатся.

Следующая политика безопасности относится к состоянию окна CTRL+ALT+DEL при входе в систему. Эта политика по умолчанию не установлена. После перезагрузки при входе в систему на экране будет отображаться окно CTRL+ALT+DEL, которое по умолчанию не отображается.

Кроме этого, в целях безопасности полезно настраивать следующие параметры:

- «Автоматически отключать сеансы пользователей по истечении разрешённого времени» (Включить);
- «Длительность простоя перед отключением сеанса» (примерно 10 мин);
- «Дополнительные ограничения для анонимных подключений» (установить в значение «Нет доступа, без явного разрешения анонимного доступа»);
- «Использовать цифровую подпись со стороны клиента (Всегда)» (Включить);
- «Использовать цифровую подпись со стороны клиента (по возможности)» (Включить);
- «Использовать цифровую подпись со стороны сервера (Всегда)» (Включить);
- «Использовать цифровую подпись со стороны сервера (по возможности)» (Включить);
- «Разрешить доступ к дисководам компакт-дисков только локальным пользователям» (Включить);
- «Разрешить доступ к НГМД только локальным пользователям» (Включить).

Брандмауэр Windows в режиме повышенной безопасности

Брандмауэр Windows в режиме повышенной безопасности – это брандмауэр, регистрирующий состояние сети, для рабочих станций. В отличие от брандмауэров для маршрутизаторов, которые развёртывают на шлюзе между локальной сетью и Интернетом, брандмауэр Windows создан для работы на отдельных компьютерах. Он отслеживает только трафик рабочей станции: трафик, приходящий на IP-адрес данного компьютера, и исходящий трафик самого компьютера. Брандмауэр Windows в режиме повышенной безопасности выполняет следующие основные операции.

Входящий пакет проверяется и сравнивается со списком разрешённого трафика. Если пакет соответствует одному из значений списка, брандмауэр Windows передает пакет протоколу TCP/IP для дальнейшей обработки. Если пакет не соответствует ни одному из значений списка, брандмауэр Windows блокирует пакет, и в том случае, если включено протоколирование, создаёт запись в файле журнала.

Список разрешённого трафика формируется двумя путями:

- когда подключение, контролируемое брандмауэром Windows в режиме повышенной безопасности, отправляет пакет, брандмауэр создаёт значение в списке разрешающее прием ответного трафика. Для соответствующего входящего трафика потребуется дополнительное разрешение;
- когда создаётся разрешающее правило брандмауэра Windows в режиме повышенной безопасности. Трафик, для которого создано соответствующее правило, будет разрешён на компьютере с работающим брандмауэром Windows. Этот компьютер будет принимать явно разрешённый входящий трафик в режимах работы в качестве сервера, клиентского компьютера или узла одноранговой сети.

Первым шагом по решению проблем, связанных с Брандмауэром Windows, является проверка того, какой профиль является активным. Брандмауэр Windows в режиме повышенной безопасности является приложением, отслеживающим сетевое окружение. Профиль брандмауэра Windows меняется при изменении сетевого окружения.

Профиль представляет собой набор настроек и правил, который применяется в зависимости от сетевого окружения и действующих сетевых подключений.

Основным нововведением в брандмауэре Windows 7 является одновременная работа нескольких сетевых профилей.

- «Общий» – публичные (общедоступные) сети, например, в кафе или аэропорт;
- «Частный» – домашние или рабочие сети;
- «Доменный» – доменная сеть в организации, определяемая автоматически.

В Windows Vista только один профиль мог быть активен в любой момент времени. Если было включено несколько профилей, наиболее безопасный из них становился активным. Например, при одновременном подключении к публичной и домашней сетям, активным становился общедоступный профиль, обеспечивающий более высокую безопасность. В Windows 7 все три профиля могут быть активны одновременно, обеспечивая соответствующий уровень безопасности для каждой сети.

Политики диспетчера списка сетей

Для того чтобы воспользоваться функционалом локальных политик безопасности, предназначенным для изменения политик списка сетей, необходимо открыть «Редактор управления групповыми политиками», в дереве консоли развернуть узел «Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики диспетчера списка сетей».

В области сведений политик диспетчера списка сетей можно настраивать:

- сети, которые не удается идентифицировать из-за ошибок сети или отсутствия идентифицируемых признаков, называемых «Неопознанные сети»;
- временное состояние сетей, находящихся в процессе идентификации, которые называются «Идентификация сетей»;
- все сети, к которым подключен пользователь, называемое «Все сети»;
- а также текущее сетевое подключение (рабочая группа или домен).

Принудительное изменение названия сетей для пользователей, находящихся в домене

Как в рабочих группах, так и в доменах пользователи могут самостоятельно изменять имя сети. Для этого нужно выполнить следующие действия:

1. Открыть окно **«Центр управления сетями и общим доступом»**;
2. В группе **«Просмотр активных сетей»** щёлкнуть на значке сети, имя которой необходимо изменить;
3. В диалоговом окне **«Настройка свойств сети»**, в текстовом поле **«Сетевое имя»** изменить имя сети.

Нужно сделать так, чтобы пользователи домена не могли изменить название сети в **«Центре управления сетями и общим доступом»**. Для этого нужно выполнить следующие действия:

1. Так как действие этой групповой политики должно распространяться на все компьютеры этого домена, в оснастке **«Управление групповой политикой»**, в дереве консоли, развернуть узел **«Лес: имя домена\Домены\имя домена»** и выбрать объект групповой политики **«Default Domain Policy»**;
2. Нажать правой кнопкой мыши на этом объекте групповой политики и из контекстного меню выбрать команду **«Изменить»**;
3. В открывшейся оснастке **«Редактор управления групповыми политиками»** в дереве консоли развернуть узел **«Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики диспетчера списка сетей»** и открыть политику **«Все**

сети». В открывшемся окне политики безопасности, в группе **«Имя сети»** установить переключатель на опцию **«Пользователь не может изменить имя»** и нажать на **«ОК»**;

4. Открыть политику, именем которой назначено имя домена. На вкладке **«Имя сети»**, в группе **«Имя»** установить переключатель на опцию **«Имя»** и указать название. В группе **«Разрешёния пользователя»** можно установить переключатель на опцию **«Пользователь не может изменить имя»**, но в этом нет крайней необходимости, так как подобная операция была выполнена на предыдущем шаге для всех сетей компьютеров организации.
5. Закрыть **«Редактор управления групповыми политиками»** и, при необходимости, обновить политики конфигурации компьютера, используя команду ***GPUpdate /Target:Computer /force /boot*** в командной строке.

Принудительное изменение профиля брандмауэра Windows в неопознанных сетях

В последние годы всё больше пользователь используют мобильные компьютеры. Используя свои мобильные компьютеры, пользователи могут подключаться к сети Интернет даже находясь в кафе, аэропортах или просто сидя на скамейке в парке. Именно в таких случаях их компьютеры находятся под более существенным риском нападения злоумышленниками, нежели в корпоративной среде или у себя дома. Когда пользователь подключается к беспроводной сети, операционная система Windows автоматически определяет такую сеть как общедоступную. Для того чтобы настройки безопасности брандмауэра Windows применялись к компьютеру в зависимости от пользовательского места нахождения были разработаны профили брандмауэра. В том случае, если соединение проходит проверку подлинности на контроллере домена, то сеть классифицируется как тип **доменного** размещения сети. Если компьютер используется дома или в офисе – обычно применяется **домашняя** сеть с **частным** профилем брандмауэра. В местах общего пользования принято использовать **общий** профиль брандмауэра. Часто случается, что пользователи, находясь в общедоступных местах, пренебрегают этим средствам безопасности и для общедоступного профиля устанавливают частные профили брандмауэра.

Используя политики диспетчера списка сетей можно указать пользователю, какой профиль нужно использовать в случае неопознанных сетей, которые идентифицируются как «Общественная сеть». Для этого выполните следующие действия:

1. Открыть оснастку **«Редактор локальной групповой политикой»**.
2. В открывшемся окне, в дереве оснастки, перейти в узел **«Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики диспетчера списка сетей»** и открыть политику **«Неопознанные сети»**.
3. В диалоговом окне **«Свойства: Неопознанные сети»,** в группе **«Тип расположения»**, установив переключатель на нужную опцию, выбрать профиль брандмауэра, который будет сопоставлен с неопознанными сетями. В данном случае, устанавливается профиль **«Общий»**. В группе **«Разрешения пользователя»** можно установить переключатель на опцию **«Пользователь не может изменить расположение»** для того чтобы пользователь вручную не мог изменить сетевое расположение.
4. Закрыть **«Редактор локальной групповой политикой»** и, при необходимости, обновить политики конфигурации компьютера, используя команду ***GPUpdate /Target:Computer /force /boot*** в командной строке.

Политики открытого ключа. Файловая система EFS

Дополнительные функции шифрованной файловой системы (Encrypting File System, EFS) обеспечили дополнительную гибкость для корпоративных пользователей при развертывании решений безопасности, основанных на шифровании файлов с данными.

Любой злоумышленник, имеющий физический доступ к компьютеру, может загрузить на нем другую ОС, обойти защиту основной ОС и получить доступ к конфиденциальным данным. Шифрование конфиденциальных файлов средствами EFS обеспечивает дополнительную защиту. Данные зашифрованного файла останутся недоступными, даже если атакующий получит полный доступ к среде хранения данных компьютера.

Только полномочные пользователи и назначенные агенты восстановления данных в состоянии расшифровывать файлы. Пользователи с другими учётными записями, обладающие разрешениями для файла – даже разрешением на передачу прав владения (Take Ownership), не в состоянии открыть его. Администратору доступ к содержимому файла также закрыт, если только он не назначен агентом восстановления данных. При попытке несанкционированного доступа к зашифрованному файлу система откажет в доступе.

Процесс шифрования в EFS

Две основные криптографические системы. Наиболее простая – шифрование с использованием секретного (симметричного) ключа, т.е. для шифровки и расшифровки данных используется один и тот же ключ. Преимущества: высокая скорость шифрования; недостатки: проблема передачи секретного ключа, а именно возможность его перехвата. Представители: DES, 3DES, DESX, AES. Отличие шифрования с открытым ключом (асимметричное шифрование) заключается в том, что данные шифруются одним ключом, а расшифровываются другим, с помощью одного и того же ключа нельзя осуществить обратное преобразование. Эта технология шифрования предполагает, что каждый пользователь имеет в своем распоряжении пару ключей – открытый ключ (public key) и личный или закрытый ключ (private key). Таким образом, свободно распространяя открытый ключ, один пользователь предоставляет другим пользователям возможность шифровать свои сообщения, направленные этому пользователю, которые сможет расшифровать только он. Если открытый ключ и попадет в «плохие руки», то он не даст возможности определить секретный ключ и расшифровать данные. Отсюда и основное преимущество систем с открытым ключом: не нужно передавать секретный ключ, однако есть и недостаток – низкая скорость шифрования. Представители: RSA, алгоритм Эль-Гамаля, алгоритм Диффи-Хелмана.

В EFS для шифрования используются все преимущества вышеперечисленных систем. Данные шифруются с помощью симметричного алгоритма с применением ключа шифрования файла (File Encryption Key, FEK). FEK – сгенерированный EFS случайным образом ключ. На следующем этапе FEK шифруется с помощью открытого ключа пользователя и сохраняется в пределах атрибута, называемого полем расшифровки данных (Data Decryption Field, DDF) непосредственно внутри самого файла. Кроме того, EFS шифрует FEK, используя открытый ключ агента восстановления, и помещает его в атрибут Data Recovery Field – DRF. DRF может содержать данные для множества агентов восстановления.

Агент восстановления данных (Data Recovery Agent, DRA) – пользователь, который имеет доступ ко всем зашифрованным данным других пользователей. Это актуально в случае утраты пользователями ключей или других непредвиденных ситуациях. Агентом восстановления данных назначается обычно администратор. Для создания агента

восстановления нужно сначала создать сертификат восстановления данных и определить политику восстановления, а затем назначить одного из пользователей таким агентом. Политика восстановления играет важную роль в системе шифрования, она определяет агентов восстановления, а их отсутствие или удаление политики вообще запрещает использование пользователями шифрования.

EFS и NTFS

Шифрованная файловая система (EFS) защищает конфиденциальные данные в файлах на томах NTFS. EFS – основная технология шифрования и расшифровки файлов на томах NTFS. Открывать файл и работать с ним может только пользователь, его зашифровавший. Это чрезвычайно важно для пользователей переносных компьютеров: даже если взломщик получит доступ к потерянному или украденному компьютеру, он не сможет открыть зашифрованные файлы. В Windows XP шифрованная файловая система также поддерживает автономные файлы и папки (Offline Files and Folders).

Зашифрованный файл останется недоступным для просмотра в исходном виде, даже если атакующий обойдет системную защиту, например, загрузив другую ОС. EFS обеспечивает устойчивое шифрование по стандартным алгоритмам и тесно интегрирована с NTFS. EFS в Windows XP предоставляет новые возможности совместного использования зашифрованных файлов или отключения агентов восстановления данных, а также облегчает управление посредством групповой политики и служебных программ командной строки.

Как работает EFS

EFS позволяет сохранить конфиденциальность информации на компьютере в условиях, когда люди, имеющие физический доступ к компьютеру, могут преднамеренно или неумышленно скомпрометировать её. EFS чрезвычайно удобна для обеспечения конфиденциальности данных на мобильных компьютерах или на компьютерах, на которых работают несколько пользователей, т. е. таких системах, которые могут подвергаться атакам, предусматривающим обход ограничений списков ACL.

В совместно используемой системе атакующий обычно получает несанкционированный доступ, загружая другую ОС. Злоумышленник также может захватить компьютер, вынуть жесткий диск, поместить его на другой компьютер и получить доступ к файлам. Однако если у него нет ключа расшифровки, зашифрованный средствами EFS файл будет выглядеть как бессмысленный набор символов.

Поскольку EFS тесно интегрирована с NTFS, шифрование и расшифровка выполняются незаметно («прозрачно») для пользователя. При открытии файла EFS автоматически расшифровывает его по мере чтения данных с диска, а при записи – шифрует данные при записи на диск.

В стандартной конфигурации EFS позволяет зашифровать файл прямо из Проводника Windows без какого-либо вмешательства администратора. С точки зрения пользователя шифрование файла или папки – это просто назначение ему определённого атрибута.

Конфигурирование EFS

По умолчанию система поддерживает работу EFS. Разрешается шифровать файлы, для которых имеется разрешение на изменение. Поскольку в EFS для шифрования файлов применяется открытый ключ, нужно создать пару ключей открытый/закрытый и сертификат с открытым ключом шифрования. В EFS разрешены сертификаты, подписанные самим владельцем, поэтому вмешательство администратора для нормальной работы не требуется.

Если применение EFS не соответствует требованиям организации или если есть файлы, которые нельзя шифровать, существует много способов отключить EFS или нужным образом конфигурировать её.

Для работы с EFS всем пользователям требуются сертификаты EFS. Если в организации нет инфраструктуры открытого ключа (Public Key Infrastructure, PKI), применяются подписанные самим владельцем сертификаты, которые автоматически создаются ОС. При наличии центров сертификации сертификаты EFS обычно выпускают именно они. Если используется EFS, необходимо предусмотреть план восстановления данных при сбое системы.

Что разрешается шифровать?

На томах NTFS атрибут шифрования разрешается назначать отдельным файлам и папкам с файлами (или подпапками). Хотя папку с атрибутом шифрования и называют «зашифрованной», сама по себе она не шифруется, и для установки атрибута пары ключей не требуется. При установленном атрибуте шифрования папки EFS автоматически шифрует:

- все новые файлы, создаваемые в папке;
- все незашифрованные файлы, скопированные или перемещённые в папку;
- все вложенные файлы и подпапки (по особому требованию);
- автономные файлы.

Политики ограниченного использования программ

Политики ограниченного использования программ предоставляют механизм идентификации программ и управления возможностями их выполнения. Существует два варианта установки правил ограничения:

- на всё программное обеспечение устанавливается ограничение на запуск и создаются исключения, то есть список программ, разрешенных к выполнению;
- разрешается запуск любых программ и создаётся список исключений, запрещающий запуск некоторых программ, доступ к программам определяется правами пользователя.

Для того чтобы выбрать один из вариантов как вариант по умолчанию, необходимо открыть пункт «Уровни безопасности» и выбрать нужный уровень. По умолчанию установлен уровень безопасности «Неограниченный», то есть запуск любых программ разрешен и необходимо создать исключения для запрета запуска определённых программ.

Политики ограниченного использования программ распространяются только на исполняемые файлы, чтобы посмотреть список таких файлов, перейдите в пункт «Назначенные типы файлов». В этот список можно добавить новый тип файлов, соответственно на такие файлы будут распространяться все установленные правила, или удалить какой-то тип, исключив такие файлы из правил политик.

По умолчанию политики распространяются на всех пользователей компьютера. Но при создании некорректных правил (например, политик ограничивающих запуск системных файлов), система может работать неправильно, при этом существует риск невозможности возвращения системы в исходное состояние. Поэтому желательно распространять действие политик только на пользователей, исключив из области действия политик локальных администраторов. Для этого перейдите в пункт «Принудительный» и выполните соответствующие настройки.

Кроме того в пункте «Принудительный» существует возможность выбора, будут ли политики распространяться на файлы библиотек *.dll. Если политики будут распространяться и на файлы *.dll, то при установке уровня безопасности по умолчанию запрещающего выполнение программ, придется создавать дополнительные разрешения

для каждой библиотеки которую использует программа, иначе программа будет работать некорректно.

С помощью политик ограниченного использования программ имеется возможность защищать компьютерное оборудование от программ неизвестного происхождения посредством определения программ, разрешенных для запуска. В данной политике приложения могут быть определены с помощью правила для хеша, правила для сертификата, правила для пути и правила для зоны Интернета. Программное обеспечение может выполняться на двух уровнях: неограниченном и запрещённом.

Политики ограниченного использования программ регулируют использование неизвестных программ и программ, к которым нет доверия. В организациях используется набор хорошо известных и проверенных приложений. Администраторы и служба поддержки обучены для поддержки этих программ. Однако, при запуске пользователем других программ, они могут конфликтовать с установленным программным обеспечением, изменять важные данные настройки или, содержать вирусы или «троянские» программы для несанкционированного удалённого доступа.

При интенсивном использовании сетей, Интернета и электронной почты в бизнесе пользователи повсеместно сталкиваются с различными программами. Пользователям постоянно приходится принимать решения о запуске неизвестных программ, поскольку документы и веб-страницы содержат программный код – сценарии. Вирусы и «троянские» программы зачастую умышленно замаскированы для введения пользователей в заблуждение при запуске. При таком большом количестве и разнообразии программ отдельным пользователям трудно определить, какое программное обеспечение следует запускать.

Пользователем необходим эффективный механизм идентификации и разделения программ на безопасные и не заслуживающие доверия. После идентификации программы к ним может быть применена политика для определения, могут ли они быть запущены. Политики ограниченного использования программ предоставляют различные способы идентификации программного обеспечения и средства определения, следует ли запускать данное приложение.

При применении политик ограниченного использования программ идентификация программного обеспечения производится посредством следующих правил:

- Правило для сертификата;

Политики ограниченного использования программ могут идентифицировать файл по его сертификату подписи. Правила для сертификатов не применяются к файлам с расширением .exe или .dll. Они используются для сценариев и пакетов установщика Windows. Имеется возможность создать правило для сертификата, идентифицирующее приложение и затем, в зависимости от уровня безопасности, позволяющее или не позволяющее его запустить. Например, администратор может использовать правила для сертификатов, чтобы автоматически доверять программам из проверенного источника в домене без запроса пользователя. Кроме того, правила для сертификатов могут использоваться в запрещённых областях операционной системы.

- Правило для пути;

Правило для пути идентифицирует программы по пути к файлу. Например, если имеется компьютер с политикой запрета по умолчанию, имеется возможность, предоставить неограниченный доступ к указанной папке для каждого пользователя. Для данного типа правил могут быть использованы некоторые общие пути: %userprofile%, %windir%, %appdata%, %programfiles% и %temp%.

Поскольку данные правила определяются с использованием пути, при перемещении программы правило для пути применяться не будет.

- Правило для хеша;

Хеш представляет собой серию байтов фиксированной длины, однозначно идентифицирующую программу или файл. Хеш рассчитывается с помощью алгоритма хеширования. Политики ограниченного использования программ могут идентифицировать файлы по их хешу с помощью алгоритмов хеширования SHA-1 (Secure Hash Algorithm) и MD5 hash algorithm.

Например, имеется возможность создать правило для хеша и задать уровень безопасности «Не разрешено», чтобы запретить запуск определённого файла. Хеш переименованного или перемещённого в другую папку файла не изменяется. Однако при любом изменении файла значение хеша изменяется, позволяя обойти ограничения.

Политики ограниченного использования программ распознают только хеши, рассчитанные с помощью политик ограниченного использования программ.

- Правило для зоны Интернета;

Правила для зоны влияют только на пакеты установщика Windows.

Правило для зоны идентифицирует программное обеспечение из зоны, указанной посредством Internet Explorer. Такими зонами являются Интернет, локальный компьютер, местная интрасеть, ограниченные узлы и надёжные сайты.

В политиках ограниченного использования программ используются следующие уровни безопасности:

- *«Неограниченный»*. Приложения запускается со всеми правами пользователя, вошедшего в систему.
- *«Не разрешено»*. Приложения не могут быть запущены.

Политики управления приложениями

AppLocker – управление правами на запуск приложений.

Одна из причин, по которой безопасность корпоративной сети организации может оказаться под угрозой, – несанкционированная установка и запуск приложений пользователями. Сотрудники могут запускать сомнительные приложения, утилиты, которые расходуют корпоративный трафик (например, Bittorent-клиенты), программы, которые вносят изменения в различные компоненты системы, что, в конечном итоге, приводит к ухудшению её производительности. Наконец, не исключена возможность запуска приложений, содержащих вредоносный код, что может стать причиной заражения компьютера вирусами.

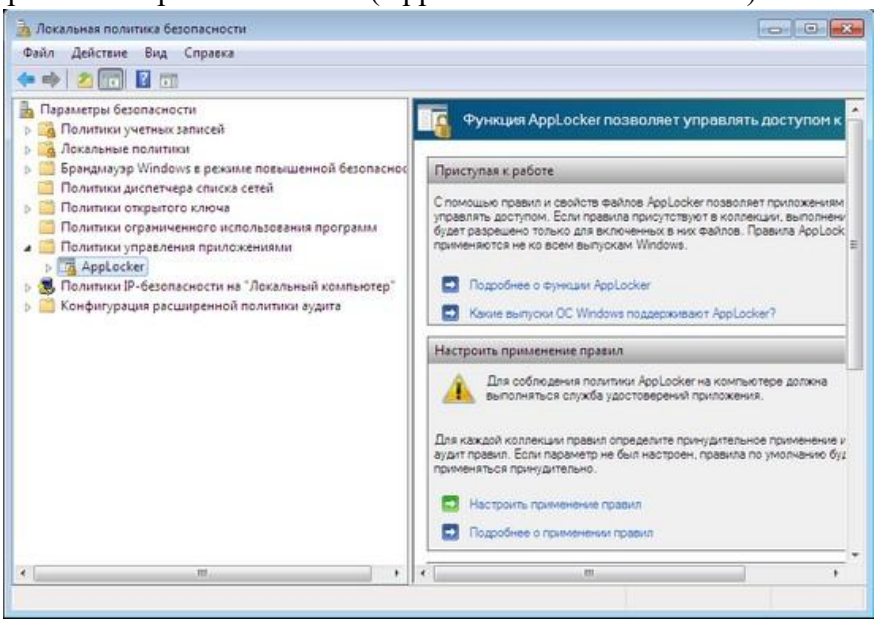
В предыдущих версиях Windows была возможность решения этой задачи при помощи политик ограниченного использования программ (Software Restriction Policies), однако этот инструмент был неудобен и несовершенен. В Windows 7 функция политик ограниченного использования программ заменена средством AppLocker, которое представляет собой изменённую и доработанную версию Software Restriction Policies.

AppLocker значительно упрощает контроль за действиями пользователей, которые касаются установки приложений, а также запуска файлов EXE, использования библиотек DLL, файлов инсталляторов MSI и MSP, а также сценариев. Основные отличия AppLocker от политик ограниченного использования программ:

- применение правила к определённому пользователю или к группе, а не только ко всем пользователям;
- мастер автоматического создания правил;
- импорт и экспорт созданных правил;

- режим «Только аудит», в котором ведется аудит приложений, которые обрабатываются правилами, однако на самом деле правила не применяются;
- условие «Издатель», которое является расширенной версией условия «Сертификаты», существовавшего ранее;
- поддержка новой командной строки Windows Power Shell;
- коллекции правил для разных типов файлов, которые не зависят друг от друга.

Для доступа к настройкам AppLocker необходимо перейти в раздел «Администрирование» (Administrative Tools) панели управления выбрать пункт «Локальная политика безопасности» (Local Security Policy), после чего раскрыть список «Политики управления приложениями» (Application Control Policies).

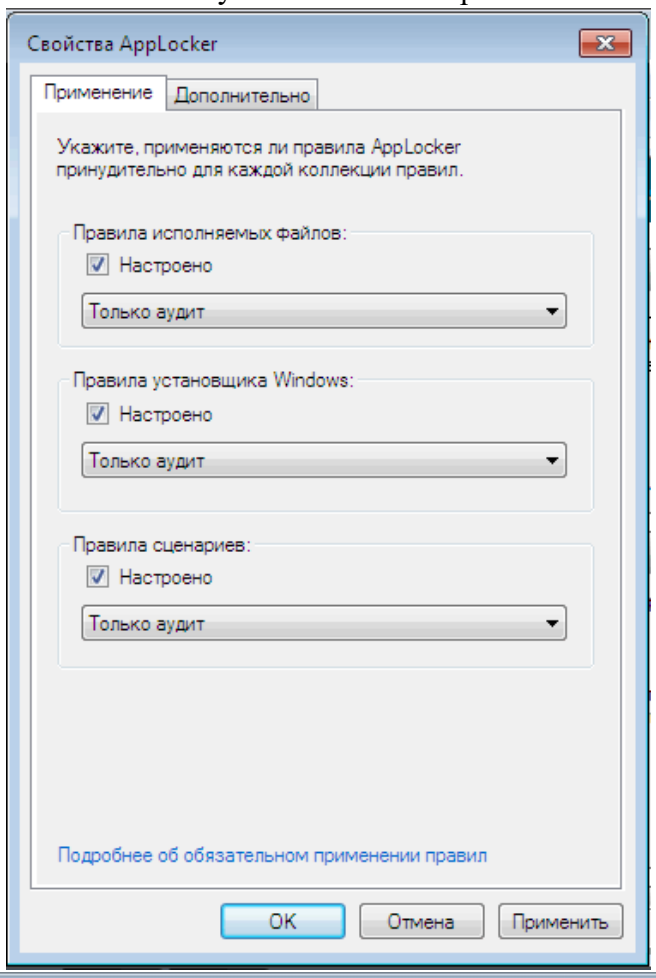


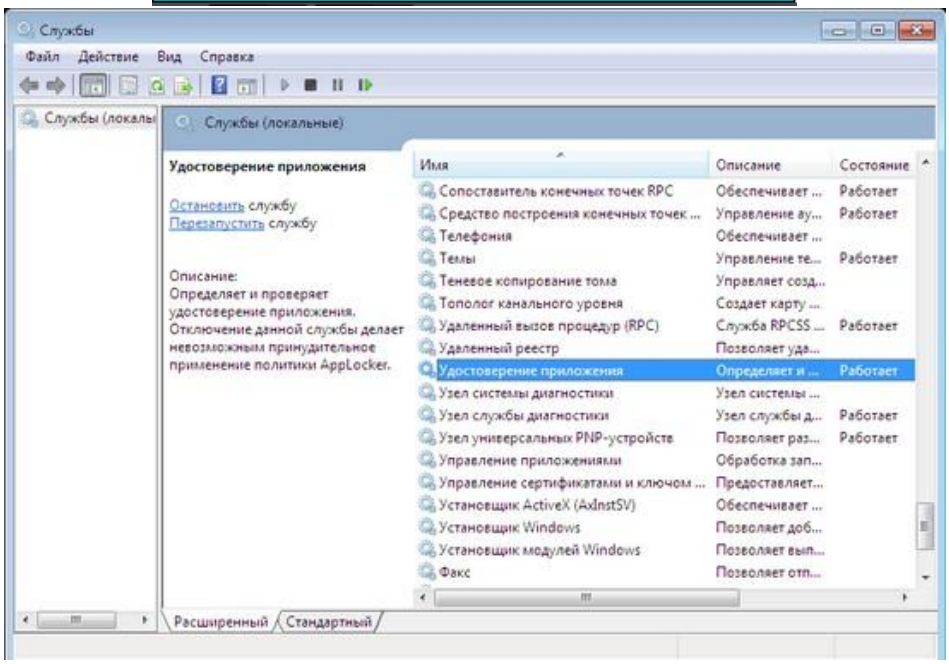
Одна из особенностей AppLocker состоит в том, что по умолчанию все правила, настроенные при помощи этого средства, применяются. Именно поэтому необходимо очень осторожно настраивать их, так как можно по неопытности заблокировать работу Windows. Во-первых, рекомендуется перед созданием правил перейти в окно их настройки, щёлкнув по ссылке «Настроить применение правил» (Configure Rule Enforcement), и для каждого типа правил (исполняемые файлы, установщик Windows и сценарии) выбрать вариант применения «Только аудит» (Audit Only). В этом случае правила с любыми настройками не смогут блокировать работу приложений или системы в целом, однако при помощи журнала событий администратор сможет просмотреть, как они применяются по отношению к файлам или приложениям. Если окажется, что правила блокируют приложения, к которым доступ должен быть разрешён, или, наоборот, не действуют на программы, к которым нужно ограничить доступ, правила можно будет отредактировать.

Второе решение, которое может помочь администраторам разобраться с новыми возможностями управления доступом, – создание и отладка правил на тестовом компьютере. AppLocker поддерживает импорт и экспорт правил, благодаря чему можно создать набор политик ограничений в безопасной среде, тщательно протестировать их работоспособность, после чего импортировать уже в рабочую среду.

Для применения правил, созданных при помощи AppLocker, необходимо, чтобы на компьютерах была запущена служба «Удостоверение приложения» (Application Identity). По умолчанию она отключена. Для её запуска откройте раздел «Администрирование» панели управления и выберите пункт «Службы», после чего

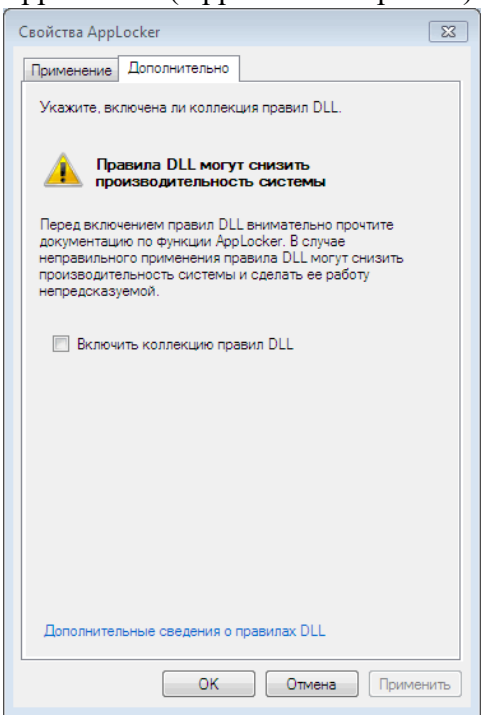
найдите службу в списке, щёлкните по её названию правой кнопкой мыши и выберите команду «Запустить». В свойствах службы можно настроить её автоматический запуск.





По умолчанию в AppLocker используется три типа (коллекции) правил, которые настраиваются и используются независимо друг от друга: исполняемые файлы (EXE и COM), установщик Windows (MSI и MSP) и сценарии (PS1, BAT, CMD, VBS и JS), однако при необходимости можно также включить правила для файлов библиотек DLL (сюда входят и файлы с расширением OCX). Для этого нужно установить флажок «Включить

коллекцию правил DLL» (Enable the DLL rule collection) на вкладке «Дополнительно» (Advanced) окна «Свойства AppLocker» (AppLocker Properties).



Стоит, однако, иметь в виду, что использование таких правил может существенно повлиять на производительность системы. Это связано с тем, что каждое приложение, как правило, использует для работы несколько файлов библиотек, поэтому на их проверку и соответствие правилам уходит гораздо больше времени, чем на проверку только приложений. Кроме этого, некоторые приложения загружают дополнительные файлы библиотек в процессе работы, поэтому проверка, которую Windows будет при этом выполнять, может замедлить работу пользователя с программой. При включении правил DLL их необходимо создавать для каждой библиотеки, которая используется всеми разрешёнными программами.

Необходимо отметить, что использование большого числа правил любого типа (это касается не только правил DLL) в любом случае будет снижать производительность системы, поскольку при попытке запуска каждого приложения Windows потребуется обрабатывать все правила, чтобы разрешить или запретить пользователю работу с программой.

Именно поэтому, создавая правила, имеет смысл строить их таким образом, чтобы общее их число было как можно меньшим. Все правила AppLocker работают по принципу разрешения («белый список»), запрета («черный список») и исключения. Иными словами, перед созданием правила стоит решить, что удобнее: 1) сделать правило, разрешающее определённое действие (при этом запуск всех приложений, которых нет в составленном администратором списке, будет запрещён), и сделать исключения для некоторых групп пользователей или приложений; или же 2) создать правило, разрешающее запускать все приложения, кроме указанных в списке, и также указать исключения.

Несмотря на то, что при помощи AppLocker можно создавать как разрешающие, так и запрещающие правила, в большинстве случаев рекомендуется использовать первый вариант. Это связано с тем, что для обеспечения безопасности любой организации гораздо логичнее составить фиксированный список разрешённых приложений, который можно по мере необходимости обновлять, нежели попытаться перечислить в правиле те программы, которые запрещено запускать. Любой новый вирус, который администратор не успел добавить в запрещающее правило, имеет все шансы проникнуть в корпоративную сеть.

Также причиной, по которой рекомендуется использовать разрешающие правила, является то, что запрещающие действия во всех случаях переопределяют разрешающие.

Для создания нового правила раскройте список AppLocker в окне «Локальная политика безопасности», необходимо щёлкнуть правой кнопкой мыши по нужному типу правила и выбрать команду «Создать новое правило». Будет запущен мастер, на первом этапе работы которого нужно будет определиться с тем, будет ли это правило разрешать или запрещать определённые действия, а также, на какие категории пользователей оно будет распространяться.

Затем нужно будет выбрать тип основного условия: «Издатель» (Publisher), «Путь» (Path) и «Хэшируемый файл» (File Hash). Несмотря на то, что типы условий похожи на те, которые использовались в политиках ограниченного использования программ в предыдущих версиях Windows, работа с ними организована по-другому.

Наиболее интересным является условие «Издатель», прототипом которого в политиках ограниченного использования программ было условие «Сертификаты» (Certificate). Это условие дает возможность разрешить запуск приложений, для которых имеется цифровая подпись издателя. При создании правил с таким условием учитывается не только название производителя, как это было в Windows XP, но и другая информация, такая как название продукта, имя файла, номер версии.

При этом условие может распространяться в точности на указанный номер версии приложения или на все версии, номер которых выше или ниже заданного. Благодаря этому, можно гибко настроить правило, которое будет разрешать установку новых версий приложений, но при этом запрещать установку старых релизов, которые могут быть несовершенны с точки зрения безопасности. Для использования условия «Издатель» нужно указать путь к файлу приложения, который содержит цифровую подпись. Установив флажок «Пользовательские значения», можно вручную отредактировать значения всех полей. Стоит иметь в виду, что если приложение не имеет цифровой подписи, то использовать условие «Издатель» в его отношении невозможно.

Условие «Путь» позволяет определить приложения, которые разрешено запускать и устанавливать пользователю, на основе их расположения в файловой системе локального компьютера, в сети или на сменных носителях. Создавая такое условие, можно использовать подстановочные знаки и переменные окружения. Например, чтобы указать путь на CD/DVD-диске, нужно использовать переменную %REMOVABLE%, а для указания пути на USB-накопителе – %HOT%.

Условие «Путь» необходимо использовать очень осторожно, так как при недостаточной продуманности оно может стать причиной того, что пользователи смогут с его помощью обходить некоторые запреты. Например, если создать разрешающее условие такого типа и включить в него расположение папки, в которую пользователь может выполнять запись, то пользователь сможет скопировать в такую папку запрещённый для запуска файл из другого расположения и запустить его.

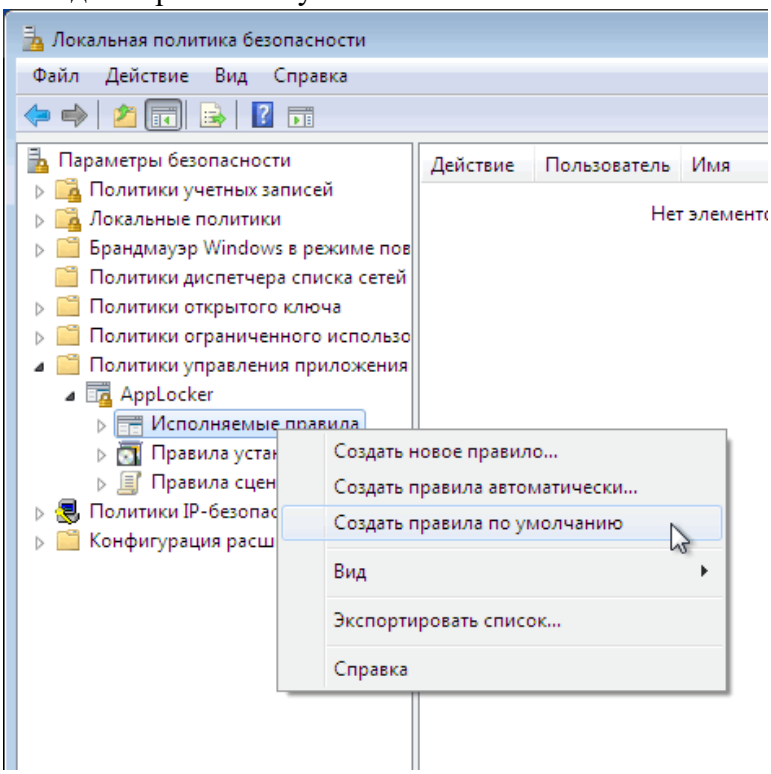
Условие «Хэшируемый файл» в большинстве случаев является наименее эффективным, так как определение легитимности файла построено на вычислении его контрольной суммы. Нетрудно догадаться, что если выходит обновление приложения, то его контрольная сумма изменяется, и условие перестает работать. С другой стороны, такой способ позволяет защититься от возможности запуска известной программы, в которую был внедрен вредоносный код. Поскольку при этом контрольная сумма изменяется, модифицированное приложение запустить будет невозможно.

Как видно, каждое из условий несовершенно и имеет свои недостатки. Именно поэтому на следующем этапе работы мастера предлагается настроить исключения.

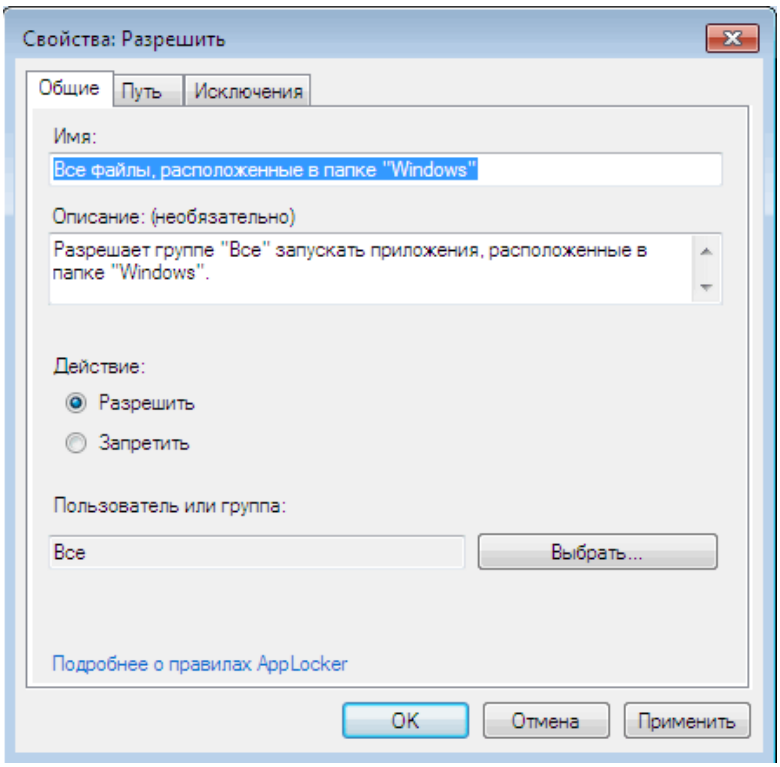
Исключения можно использовать, если в качестве основного выбраны условия «Издатель» и «Путь».

Наконец, на последнем этапе работы мастера нужно дать правилу название, а также снабдить его описанием. Несмотря на то, что последнее необязательно, не стоит пренебрегать этой возможностью, так как описание может помочь в будущем вспомнить, за что отвечает то или иное правило.

Чтобы лучше понять, как работают правила, можно начать с создания правил по умолчанию. Они доступны для каждого из типов правил. Например, правила для исполняемых файлов включают такие: разрешение на запуск любых приложений членам группы «Администраторы», разрешение на запуск приложений, находящихся в директории Program Files и в папке Windows, для членов группы «Все». Для создания набора правил по умолчанию нужно раскрыть список AppLocker в окне «Локальная политика безопасности», щёлкнуть правой кнопкой мыши по нужному типу правила и выбрать команду «Создать правила по умолчанию».



Правила по умолчанию можно редактировать. Для этого нужно щёлкнуть по названию правила в списке и выбрать строку «Свойства». Редактировать можно все свойства правил, например, добавлять исключения, изменять пути, группы пользователей, на которые они распространяются, и т.д.



В AppLocker встроен автоматический механизм, упрощающий создание правил. Выберите команду «Создать правила автоматически» для определённого типа правил, укажите группы пользователей, к которым будут применяться создаваемые правила, а также папку, в которую установлены приложения.

При автоматическом создании правил мастер пытается максимально уменьшить их число. В таком режиме создаются только разрешающие правила. Если среди проанализированных приложений имеются такие, которые созданы одним разработчиком и у которых совпадает название продукта (согласно цифровой подписи), для них создаётся одно правило с условием «Издатель». Что касается условия «Хеш», то создаётся одно условие, которое содержит контрольные суммы всех файлов.

После завершения работы мастера автоматического создания правил AppLocker выдает отчет, в котором выводит общее количество файлов и число правил, которые будут созданы. Перед созданием правил есть возможность просмотреть как проанализированные файлы, так и составленные правила.

Используя AppLocker, нужно иметь в виду, что правила, созданные с его помощью, могут быть применены только на компьютерах, работающих под управлением Windows 7 Максимальная, Windows 7 Корпоративная и Windows Server 2008 R2.

Политики безопасности IP на «Локальный компьютер

После стандартной инсталляции в операционной системе предлагаются три варианта настройки для организации защищенного IP-канала – политики безопасности IPSec в рамках одного домена:

- «Сервер» – для всего трафика IP всегда запрашивает безопасность с помощью доверия Kerberos. Разрешает небезопасную связь с клиентами, которые не отвечают на запрос;
- «Безопасность сервера» – для всего IP-трафика всегда запрашивает безопасность с помощью доверия Kerberos. Не разрешает небезопасную связь с недоверенными клиентами;

- «Клиент» – обычная связь (небезопасная). Использует правило ответа по умолчанию для согласования с серверами, запрашивающими безопасность. Только запрошенный протокол и трафик с этим сервером будут безопасными.

После установки операционной системы ни одна из политик не назначена. Пользователь может активизировать (назначить) одну и только одну из существующих политик.

Ниже, в качестве справочной информации, приводятся настройки, которые используются Microsoft для трех стандартных вариантов политики безопасности IPSec.

При изучении вопросов, связанных с установлением защищенного соединения IPSec индивидуальные рекомендации необходимы для случая, если компьютер, который необходимо задействовать в схеме защищенного соединения, имеет несколько IP-адресов. Кроме того, для случая работы в домене локальная политика безопасности компьютера может перекрываться политикой безопасности, определяемой контроллером домена.

Назначение и отключение IPSec-соединения с использованием стандартных настроек Windows

Для организации аутентифицированного и закрытого обмена данными между двумя компьютерами по протоколу IPSec необходимо активизировать на одной стороне политику «Безопасность сервера», на другой – «Клиент» в разделе «Политики безопасности IP на Локальный компьютер». Это можно сделать, выбрав пункт локального меню (вызываемого по правой кнопке «мыши») «Назначить», предварительно выбрав строку с нужной политикой.

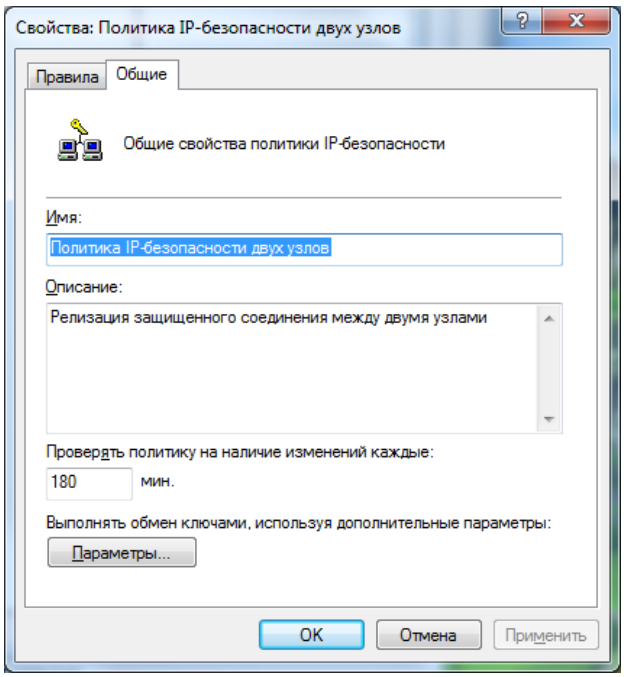
Стандартные политики предназначены для использования в рамках одного домена. В противном случае защищённое соединение не будет установлено.

Связывающиеся стороны должны быть уверены, что настройки используемых политик остались неизменными с момента установки операционной системы. Вместе с тем теоретически существует ненулевая вероятность, что после выполнения согласования поддерживаемых криптографических алгоритмов и ключевых данных, соединение будет организовано только с использованием протокола аутентификации, которое предполагает активизацию механизмов только авторства и целостности передаваемых пакетов, в то время как само содержимое пакетов будет передаваться по сети в открытом виде. Это создаёт предпосылки к тому, что все данные, которыми обмениваются компьютеры, организовавшие «защищенный» канал, будут перехвачены.

Чтобы удалить назначение политики IPSec, нужно щёлкнуть на активной политике правой кнопкой «мыши» и выбрать команду «Снять». Кроме того, можно отключить на компьютере службу «Агент политики IPSEC». Это позволит обеспечить гарантированное отключение использования политики безопасности IPSec, которая может управляться на уровне контроллера домена.

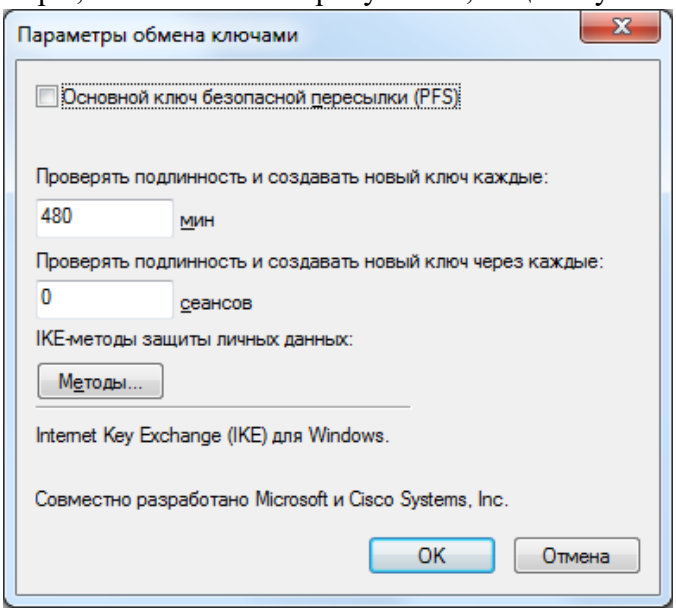
Редактирование общих настроек политики безопасности IP

Необходимо выберать закладку «Общие» в окне «Свойства».



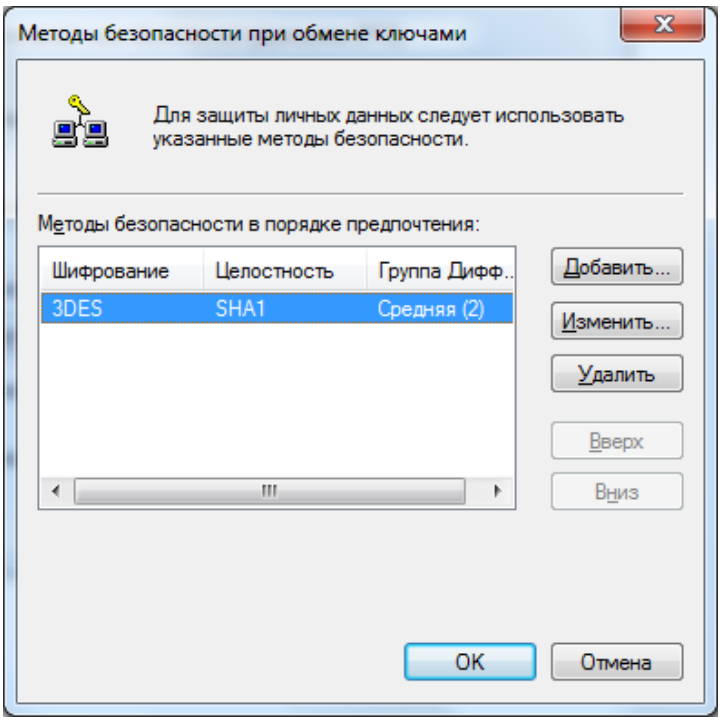
В поле «Проверять политику на наличие изменений каждые: « должно быть записано значение 180 мин., щёлкнуть кнопку «Дополнительно...». При этом открывается окно «Параметры обмена ключами».

Установить параметры, как показано на рисунке 11, и щёлкнуть «Методы».



При этом откроется окно «Методы безопасности при обмене ключами», в котором нужно удалить все строки, кроме одной с параметрами:

- «Тип (Type)» – IKE;
- «Шифрование (Encryption)» – 3DES;
- «Целостность (Integrity)» – SHA1;
- «Группа Диффи-Хелмана (Diffie-Hellman ...)» – Средняя (2).



Настройки новой политики безопасности IP

Для настройки новой политики ниже будет подробно описана последовательность действий, определяемая следующими шагами:

1. Создание новой политики безопасности IP.
2. Определение нового правила:

- списка IP-фильтров (назначение используемых сетевых протоколов и адресов взаимодействующих хостов);
- действия фильтра (выбор используемых криптографических алгоритмов);
- методов проверки подлинности (назначение способа установления доверительных отношений между компьютерами);
- типа подключения (удалённый доступ, локальная сеть);
- параметров туннеля (использовать или нет туннельный вариант протокола IPSec).

Практическое занятие № 43-44

Тема: Модификация объекты защиты, категории, технологии защиты в DLP – системе.

Практическая часть 1:

Моделирование объекта защиты

Цель: Анализ характеристик защищаемого объекта, определение задач и функций СФЗ.

Задачи.

1) Описание объекта защиты, характеристика назначения объекта.

2) Построение структурной модели конфиденциальной информации.

3) Разработка граф-структуры защищаемой информации.

4) Определение категории защищаемой информации.

5) Определение задач и функций СФЗ.

6) Формулирование принципов построения СФЗ.

Описание объекта защиты

Задание 1.

1) Параметры объекта. В соответствии с вариантом задания определить границы территории объекта, описать расположение здания, планировку здания и определить все

точки доступа на территорию объекта. Разработать план помещений объекта, описать расположение оборудования, заполнить таблицу 2.1.

Таблица 2.1 – Описание объекта защиты

	Наименование параметра	Данные
	Площадь, кв.м.	
	Высота потолка.	
	Толщина стен: наружных, внутренних.	
	Окна: количество, размер.	
	Двери: размер проема, тип, замок.	
	Описание смежных помещений: сверху, сбоку слева, сбоку справа, снизу.	
	Система электропитания (освещение): тип светильников и их количество.	
	Система заземления.	
	Системы сигнализации.	
0	Система вентиляции (тип).	
1	Наличие экранов на батареях.	
2	Телефонные линии: городская сеть, тип розеток.	

2) Описание рабочих процессов на объекте. Привести описание ведущихся на объекте работ, дать характеристику операций, выполняемых на объекте и условий их выполнения. Сформулировать назначение объекта.

3) Описание обстановки вокруг объекта. Провести анализ месторасположения объекта (в какой части города расположен объект), какие объекты находятся в ближайшем окружении. Составить пространственную модель объекта по примеру таблицы 2.2.

Таблица 2.2 - Пространственная модель контролируемых зон

п.п	Пространственная характеристика помещения	**Функциональная, конструктивная и техническая характеристика помещения**		
	Этаж	2	Площадь, $м^2$	56
	Количество окон, тип сигнализации, наличие штор на окнах	3 окна, жалюзи на окнах, плотные шторы, датчики разбития стекла «Breakglass 2000», F2, Y2, M1:2	Куда выходят окна	Проспект Сталинграда
	Двери, кол-во, одинарные, двойные	4 двери звукоизолирующие тяжелые	Куда выходят двери	Коридор, каб. №3, каб. №2, каб. №1

	Соседние помещения, название, толщина стен	1.С западной стороны находится Помещение №3. отштукатуренная с двух сторон стена (толщина - 1,5 кирпича) 2. С восточной стороны расположен коридор. отштукатуренная с двух сторон стена (толщина - 1,5 кирпича)

Построение структурной модели конфиденциальной информации

Для создания полной модели объекта защиты необходимо проанализировать защищаемую информацию и провести её структурирование.

Практическая часть 2:

Изучение функционала и областей применения DLP систем на примере InfoWatch TrafficMonitor или других аналогов

Цель: изучение функционала и областей применения DLP систем на примере InfoWatch Traffic Monitor или других аналогов.

Теоретические вопросы

1. Назначение InfoWatch Traffic Monitor.
2. Возможности InfoWatch Traffic Monitor.
3. Архитектура системы InfoWatch Traffic Monitor.
4. Общие принципы анализа данных.
5. Мониторинг и обработка данных.

Задание 1. Опишите основные функции InfoWatch Traffic Monitor.

Задание 2. Опишите компоненты системы InfoWatch Traffic Monitor

Компонент	Назначение
Traffic Monitor Server включает в себя отдельные подсистемы для контроля различных видов трафика а также подсистемы анализа: Decision and Analysis Engine (DAE) (интегрирована с подсистемами контроля), Content Analysis Server (CAS)	
Sniffer	
Management Console	
CreateSchemaWizard	

Задание 3. Опишите варианты настройки приложения InfoWatch Traffic Monitor.

Практическое занятие № 45-46

Тема: Применение политики для контроля трафика, выявления и блокирования инцидентов безопасности

Практическая часть:

1. Запустить консоль «Локальные политика безопасности», перейти к настройке «Политике учётных записей».
2. Перейти к пункту «Пороговое значение блокировки» в «Политике блокировки учётной записи», установить параметр равный 3 попыткам.
3. Перейти к пункту «Минимальная длина пароля» в «Политике паролей», установить значение 10.

4. Перейти к пункту «Пароль должен отвечать требованиям сложности», поставить галочку.

Длина пароля может достигать 128 знаков. Маленький отрывок из поэмы А.С.Пушкина «Руслан и Людмила» со всеми знаками препинания, набранный русскими буквами в латинской раскладке и установленный в качестве пароля, может привести в замешательство любого взломщика: E kerjvjhmz le, ptktysq, Pkfnfz wtgm yf le,t njv, B lytv b yjxm. Rjn extysq, Dct [jlbn gj wtgb rheujv/. Этот пароль надежный, а запомнить его очень просто: «У лукоморья дуб зеленый, златая цепь на дубе том, и днём и ночью кот учёный, всё ходит по цепи кругом».

Кроме того, специалистами были разработаны рекомендации по созданию усиленных паролей, использование которых уменьшает вероятность успешной атаки взломщика:

- пароль должен содержать не менее 6 символов, и среди них должны быть символы по крайней мере трех типов из следующих четырех: заглавные буквы, строчные буквы, цифры и специальные символы (то есть ,%,*,&,!)
- пароль не может включать учётное имя пользователя;
- если пользователь создаёт пароль, который не отвечает перечисленным требованиям, операционная система выдает сообщение об ошибке и не принимает пароль.

5. Проверить действие установленных настроек.

Политика аудита

В процессе аудита используются три средства управления: политика аудита, параметры аудита в объектах, а также журнал **«Безопасность»**, куда заносятся события, связанные с безопасностью, такие как вход/выход из системы, использование привилегий и обращение к ресурсам.

Политика аудита настраивает в системе определённого пользователя и группы аудит активности. Для того чтобы отконфигурировать политики аудита, в редакторе управления групповыми политиками необходимо открыть узел **«Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Локальные политики /Политика аудита»**. Необходимо помнить, что по умолчанию параметр политики аудита, для рабочих станций установлен на **«Не определено»**. В общей сложности, возможна настройка девяти политик аудита.

Так же, как и с остальными политиками безопасности, для настройки аудита нужно определить параметр политики. После двойного нажатия левой кнопкой мыши на любом из параметров, установите флажок на опции **«Определить следующие параметры политики»** и укажите параметры ведения аудита успеха, отказа или обоих типов событий.

После настройки политики аудита события будут заноситься в журнал безопасности. Просмотреть эти события можно в журнале безопасности.

Аудит входа в систему. Текущая политика определяет, будет ли операционная система пользователя, для компьютера которого применяется данная политика аудита, выполнять аудит каждой попытки входа пользователя в систему или выхода из неё. Например, при удачном входе пользователя на компьютер генерируется событие входа учётной записи. События выхода из системы создаются каждый раз, когда завершается сеанс вошедшей в систему учётной записи пользователя. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Аудит доступа к объектам. Данная политика безопасности выполняет аудит попыток доступа пользователей к объектам, которые не имеют отношения к Active

Directory. К таким объектам можно отнести файлы, папки, принтеры, разделы системного реестра, которые задаются собственными списками в системном списке управления доступом (SACL). Аудит создаётся только для объектов, для которых указаны списки управления доступом, при условии, что запрашиваемый тип доступа и учётная запись, выполняющая запрос, соответствуют параметрам в данных списках.

Аудит доступа к службе каталогов. При помощи этой политики безопасности можно определить, будет ли выполняться аудит событий, указанных в системном списке контроля доступа (SACL), который можно редактировать в диалоговом окне **«Дополнительные параметры безопасности»** свойств объекта Active Directory. Аудит создаётся только для объектов, для которых указан системный список управления доступом, при условии, что запрашиваемый тип доступа и учётная запись, выполняющая запрос, соответствуют параметрам в данном списке. Данная политика в какой-то степени похожа на политику **«Аудит доступа к объектам»**. Аудит успехов означает создание записи аудита при каждом успешном доступе пользователя к объекту Active Directory, для которого определена таблица SACL. Аудит отказов означает создание записи аудита при каждой неудачной попытке доступа пользователя к объекту Active Directory, для которого определена таблица SACL.

Аудит изменения политики. Эта политика аудита указывает, будет ли операционная система выполнять аудит каждой попытки изменения политики назначения прав пользователям, аудита, учётной записи или доверия. Аудит успехов означает создание записи аудита при каждом успешном изменении политик назначения прав пользователей, политик аудита или политик доверительных отношений. Аудит отказов означает создание записи аудита при каждой неудачной попытке изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Аудит изменения привилегий. Используя эту политику безопасности, можно определить, будет ли выполняться аудит использования привилегий и прав пользователей. Аудит успехов означает создание записи аудита для каждого успешного применения права пользователя. Аудит отказов означает создание записи аудита для каждого неудачного применения права пользователя.

Аудит отслеживания процессов. Текущая политика аудита определяет, будет ли операционная система выполнять аудит событий, связанных с процессами, такими как создание и завершение процессов, а также активация программ и непрямой доступ к объектам. Аудит успехов означает создание записи аудита для каждого успешного события, связанного с отслеживаемым процессом. Аудит отказов означает создание записи аудита для каждого неудачного события, связанного с отслеживаемым процессом.

Аудит системных событий. Данная политика безопасности имеет особую ценность, так как именно при помощи этой политики можно узнать, перегружался ли у пользователя компьютер, превысил ли размер журнала безопасности пороговое значение предупреждений, была ли потеря отслеженных событий из-за сбоя системы аудита и даже вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени. Аудит успехов означает создание записи аудита для каждого успешного системного события. Аудит отказов означает создание записи аудита для каждого неудачного завершения системного события.

Аудит событий входа в систему. При помощи этой политики аудита можно указать, будет ли операционная система выполнять аудит каждый раз при проверке данным компьютером учётных данных. При использовании этой политики создаётся событие для локального и удаленного входа пользователя в систему. Члены домена и компьютеры, не входящие в домен, являются доверенными для своих локальных учётных

записей. Когда пользователь пытается подключиться к общей папке на сервере, в журнал безопасности записывается событие удалённого входа (события выхода из системы не записываются). Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Аудит управления учётными записями. Эта последняя политика тоже считается очень важной, так как именно при помощи неё можно определить, необходимо ли выполнять аудит каждого события управления учётными записями на компьютере. В журнал безопасности будут записываться такие действия как создание, перемещение и отключение учётных записей, а также изменение паролей и групп. Аудит успехов означает создание записи аудита для каждого успешного события управления учётными записями. Аудит отказов означает создание записи аудита для каждого неудачного события управления учётными записями

Политики назначения прав пользователей

Как говорилось выше, для назначения прав пользователей существует 44 политики безопасности. Далее можно ознакомиться с восемнадцатью политиками безопасности, которые отвечают за назначение различных прав для пользователей или групп вашей организации.

1. **Архивация файлов и каталогов**. При помощи данной политики можно указать пользователей или группы, предназначенные для выполнения операций резервного копирования файлов, каталогов, разделов реестра и других объектов, которые подлежат архивации. Данная политика предоставляет доступ для следующих разрешений:
   - обзор папок/выполнение файлов;
   - содержимое папки/чтение данных;
   - чтение атрибутов;
   - чтение расширенных атрибутов;
   - чтение разрешений.

   На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**, а на контроллерах домена – **«Операторы архивации»** и **«Операторы сервера»**.
2. **Блокировка страниц в памяти**. Используя эту политику безопасности, можно указать конкретных пользователей или группы, которым разрешается использовать процессы для сохранения данных в физической памяти для предотвращения сброса данных в виртуальную память на диске.

   По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.
3. **Восстановление файлов и каталогов**. Эта политика позволяет указывать пользователей и группы, которые могут выполнять восстановление файлов и каталогов, в обход блокировке файлов, каталогов, разделов реестра и прочих объектов, расположенных в архивных версиях файлов.

   На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**, а на контроллерах домена – **«Операторы архивации»** и **«Операторы сервера»**.
4. **Вход в качестве пакетного задания**. При создании задания, используя планировщик заданий, операционная система регистрирует пользователя в системе как пользователя с пакетным входом. Данная политика разрешает группе или определённому пользователю входить в систему при помощи такого метода.

По умолчанию, как на рабочих станциях, так и на контроллерах домена, данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**.

5. **Вход в качестве службы**. Некоторые системные службы осуществляют вход в операционную систему под разными учётными записями. Например, служба **«Windows Audio»** запускается под учётной записью **«Локальная служба»**, служба **«Телефония»** использует учётную запись **«Сетевая служба»**. Данная политика безопасности определяет, какие учётные записи служб могут зарегистрировать процесс в качестве службы.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

6. **Выполнение задач по обслуживанию томов**. Используя эту политику, можно указать пользователей или группы, участники которых могут выполнять операции, предназначенные для обслуживания томов. У пользователей, обладающих такими привилегиями, есть права на чтение и изменение запрошенных данных после открытия дополнительных файлов, они также могут просматривать диски и добавлять файлы в память, занятую другими данными.

По умолчанию, такими правами обладают только администраторы рабочих станций и контроллеров домена.

7. **Добавление рабочих станций к домену**. Эта политика отвечает за разрешение пользователям или группам добавлять компьютеры в домен Active Directory. Пользователь, обладающий данными привилегиями, может добавить в домен до десяти компьютеров.

По умолчанию, все пользователи, прошедшие проверку подлинности, на контроллерах домена могут добавлять до десяти компьютеров.

8. **Доступ к диспетчеру учётных данных от имени доверенного вызывающего**. Диспетчер учётных данных – это компонент, который предназначен для хранения учётных данных, таких как имена пользователей и пароли, используемых для входа на веб-сайты или другие компьютеры в сети. Эта политика используется диспетчером учётных данных в ходе архивации и восстановления, и её не желательно предоставлять пользователям.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

9. **Доступ к компьютеру из сети**. Данная политика безопасности отвечает за разрешение подключения к компьютеру по сети указанным пользователям или группам.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**, **«Пользователи»** и **«Все»**. На контроллерах домена – **«Администраторы»**, **«Проверенные пользователи»**, **«Контроллеры домена предприятия»** и **«Все»**.

10. **Завершение работы системы**. Используя этот параметр политики, можно составить список пользователей, которые имеют право на использование команды **«Завершение работы»** после удачного входа в систему.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»**, **«Операторы архивации»** и **«Пользователи»** (только на рабочих станциях), а на контроллерах домена – **«Администраторы»**, **«Операторы архивации»**, **«Операторы сервера»** и **«Операторы печати»**.

11. **Загрузка и выгрузка драйверов устройств**. При помощи текущей политики можно указать пользователей, которым будут предоставлены права на динамическую загрузку и выгрузку драйверов устройств в режиме ядра.

Эта политика не распространяется на PnP-устройства. **Plug and Play** – технология, предназначенная для быстрого определения и конфигурирования устройств в компьютере и других технических устройствах. Разработана фирмой Microsoft при содействии других компаний. Технология PnP основана на использовании объектно-ориентированной архитектуры, ее объектами являются внешние устройства и программы. Операционная система автоматически распознает объекты и вносит изменения в конфигурацию абонентской системы.).

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»**, а на контроллерах домена – **«Администраторы»** и **«Операторы печати»**.

12. **Замена маркера уровня процесса**. Используя данную политику безопасности, можно ограничить пользователей или группу от использования API-функции CreateProcessAsUser для того, чтобы одна служба могла запускать другую функцию, процесс или службу. Стоит обратить внимание на то, что такое приложение как **«Планировщик заданий»** для своей работы использует данные привилегии.

По умолчанию, как на рабочих станциях, так и на контроллерах домена, данные привилегии предоставляются учётным записям **«Сетевая служба»** и **«Локальная служба»**.

13. **Запретить вход в систему через службу удалённых рабочих столов**. При помощи данной политики безопасности можно ограничить пользователей или группы от входа в систему в качестве клиента удалённых рабочих столов.

По умолчанию, как на рабочих станциях, так и на серверах, всем разрешено входить в систему как клиенту удалённых рабочих столов.

14. **Запретить локальный вход**. Данная политика запрещает отдельным пользователям или группам выполнять вход в систему.

По умолчанию всем пользователям разрешен вход в систему.

15. **Изменение метки объектов**. Благодаря данной политике назначения прав, можно предоставить возможность указанным пользователям или группам изменять метки целостности объектов других пользователей, таких как файлы, разделы реестра или процессы.

По умолчанию никому не разрешено изменять метки объектов.

16. **Изменение параметров среды изготовителя**. Используя эту политику безопасности, можно указать пользователей или группы, которым будет доступна возможность чтения переменных аппаратной среды. Переменные аппаратной среды – это параметры, сохраняемые в энергонезависимой памяти компьютеров, архитектура которых отлична от x86.

На рабочих станциях и контроллерах домена, по умолчанию данные привилегии предоставляются группам **«Администраторы»**.

17. **Изменение системного времени**. Эта политика отвечает за изменение системного времени. Предоставив данное право пользователям или группам, тем самым кроме разрешения изменения даты и времени внутренних часов предоставляется возможность изменения соответствующего времени отслеживаемых событий в оснастке **«Просмотр событий»**.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Локальная служба»**, а на контроллерах домена – **«Администраторы»**, **«Операторы сервера»** и **«Локальная служба»**.

18. **Изменение часового пояса**. При помощи текущей политики безопасности, можно указать пользователей или группы, которым разрешено изменять часовой пояс своего компьютера для отображения местного времени, которое представляет собой сумму системного времени компьютера и смещения часового пояса.

На рабочих станциях и контроллерах домена по умолчанию данные привилегии предоставляются группам **«Администраторы»** и **«Пользователи»**.

Параметры безопасности

Узел «Параметры безопасности» позволяет администратору безопасности вручную настраивать уровни безопасности, назначенные политике локального компьютера. Чтобы изменить любое из значений шаблона, необходимо дважды щёлкнуть его. Появится диалоговое окно, позволяющее модифицировать значение.

Таким образом контролировать включение или отключение настроек безопасности, таких как цифровая подпись данных, имена учётных записей администратора и гостя, доступ к дисководам гибких и компакт-дисков, установка драйверов и приглашения на вход в систему и все остальные доступные параметры политики безопасности. Далее будут рассмотрены подробнее, какие параметры рекомендуется устанавливать для повышения защиты компьютера от различного рода атак по сети Интернет.

Первое – напоминать пользователям об истечении срока действия пароля – 14 дней (по умолчанию).

Рекомендуется включать политику «Не отображать последнего имени пользователя в диалоге входа» (по умолчанию – отключен). Особенно полезно в случае, когда рядовой пользователь имеет пароль аналогичный своему имени, и тогда без труда можно с нескольких переборов пароля хакеру проникнуть на этот компьютер.

Рекомендуется включать политику «Запретить пользователям установку драйвера принтера» (по умолчанию – отключен). А также рекомендуется включить политику «Очистка страничного файла виртуальной памяти» (по умолчанию – отключен). После этого система всегда при выключении компьютера будет удалять файл подкачки. Но здесь есть свой недостаток – система будет долго выключатся.

Следующая политика безопасности относится к состоянию окна CTRL+ALT+DEL при входе в систему. Эта политика по умолчанию не установлена. После перезагрузки при входе в систему на экране будет отображаться окно CTRL+ALT+DEL, которое по умолчанию не отображается.

Кроме этого, в целях безопасности полезно настраивать следующие параметры:

- «Автоматически отключать сеансы пользователей по истечении разрешённого времени» (Включить);
- «Длительность простоя перед отключением сеанса» (примерно 10 мин);
- «Дополнительные ограничения для анонимных подключений» (установить в значение «Нет доступа, без явного разрешения анонимного доступа»);
- «Использовать цифровую подпись со стороны клиента (Всегда)» (Включить);
- «Использовать цифровую подпись со стороны клиента (по возможности)» (Включить);
- «Использовать цифровую подпись со стороны сервера (Всегда)» (Включить);
- «Использовать цифровую подпись со стороны сервера (по возможности)» (Включить);

- «Разрешить доступ к дисководам компакт-дисков только локальным пользователям» (Включить);
- «Разрешить доступ к НГМД только локальным пользователям» (Включить).

Брандмауэр Windows в режиме повышенной безопасности

Брандмауэр Windows в режиме повышенной безопасности – это брандмауэр, регистрирующий состояние сети, для рабочих станций. В отличие от брандмауэров для маршрутизаторов, которые развёртывают на шлюзе между локальной сетью и Интернетом, брандмауэр Windows создан для работы на отдельных компьютерах. Он отслеживает только трафик рабочей станции: трафик, приходящий на IP-адрес данного компьютера, и исходящий трафик самого компьютера. Брандмауэр Windows в режиме повышенной безопасности выполняет следующие основные операции.

Входящий пакет проверяется и сравнивается со списком разрешённого трафика. Если пакет соответствует одному из значений списка, брандмауэр Windows передает пакет протоколу TCP/IP для дальнейшей обработки. Если пакет не соответствует ни одному из значений списка, брандмауэр Windows блокирует пакет, и в том случае, если включено протоколирование, создаёт запись в файле журнала.

Список разрешённого трафика формируется двумя путями:

- когда подключение, контролируемое брандмауэром Windows в режиме повышенной безопасности, отправляет пакет, брандмауэр создаёт значение в списке разрешающее прием ответного трафика. Для соответствующего входящего трафика потребуется дополнительное разрешение;
- когда создаётся разрешающее правило брандмауэра Windows в режиме повышенной безопасности. Трафик, для которого создано соответствующее правило, будет разрешён на компьютере с работающим брандмауэром Windows. Этот компьютер будет принимать явно разрешённый входящий трафик в режимах работы в качестве сервера, клиентского компьютера или узла одноранговой сети.

Первым шагом по решению проблем, связанных с Брандмауэром Windows, является проверка того, какой профиль является активным. Брандмауэр Windows в режиме повышенной безопасности является приложением, отслеживающим сетевое окружение. Профиль брандмауэра Windows меняется при изменении сетевого окружения. Профиль представляет собой набор настроек и правил, который применяется в зависимости от сетевого окружения и действующих сетевых подключений.

Основным нововведением в брандмауэре Windows 7 является одновременная работа нескольких сетевых профилей.

- «Общий» – публичные (общедоступные) сети, например, в кафе или аэропорт;
- «Частный» – домашние или рабочие сети;
- «Доменный» – доменная сеть в организации, определяемая автоматически.

В Windows Vista только один профиль мог быть активен в любой момент времени. Если было включено несколько профилей, наиболее безопасный из них становился активным. Например, при одновременном подключении к публичной и домашней сетям, активным становился общедоступный профиль, обеспечивающий более высокую безопасность. В Windows 7 все три профиля могут быть активны одновременно, обеспечивая соответствующий уровень безопасности для каждой сети.

Политики диспетчера списка сетей

Для того чтобы воспользоваться функционалом локальных политик безопасности, предназначенным для изменения политик списка сетей, необходимо открыть «Редактор управления групповыми политиками», в дереве консоли развернуть узел «Конфигурация

компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики диспетчера списка сетей».

В области сведений политик диспетчера списка сетей можно настраивать:

- сети, которые не удается идентифицировать из-за ошибок сети или отсутствия идентифицируемых признаков, называемых «Неопознанные сети»;
- временное состояние сетей, находящихся в процессе идентификации, которые называются «Идентификация сетей»;
- все сети, к которым подключен пользователь, называемое «Все сети»;
- а также текущее сетевое подключение (рабочая группа или домен).

Принудительное изменение названия сетей для пользователей, находящихся в домене

Как в рабочих группах, так и в доменах пользователи могут самостоятельно изменять имя сети. Для этого нужно выполнить следующие действия:

1. Открыть окно **«Центр управления сетями и общим доступом»**;
2. В группе **«Просмотр активных сетей»** щёлкнуть на значке сети, имя которой необходимо изменить;
3. В диалоговом окне **«Настройка свойств сети»**, в текстовом поле **«Сетевое имя»** изменить имя сети.

Нужно сделать так, чтобы пользователи домена не могли изменить название сети в **«Центре управления сетями и общим доступом»**. Для этого нужно выполнить следующие действия:

1. Так как действие этой групповой политики должно распространяться на все компьютеры этого домена, в оснастке **«Управление групповой политикой»**, в дереве консоли, развернуть узел **«Лес: имя домена\Домены\имя домена»** и выбрать объект групповой политики **«Default Domain Policy»**;
2. Нажать правой кнопкой мыши на этом объекте групповой политики и из контекстного меню выбрать команду **«Изменить»**;
3. В открывшейся оснастке **«Редактор управления групповыми политиками»** в дереве консоли развернуть узел **«Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики диспетчера списка сетей»** и открыть политику **«Все сети». В** открывшемся окне политики безопасности, в группе **«Имя сети»** установить переключатель на опцию **«Пользователь не может изменить имя»** и нажать на **«ОК»**;
4. Открыть политику, именем которой назначено имя домена. На вкладке **«Имя сети»**, в группе **«Имя»** установить переключатель на опцию **«Имя»** и указать название. В группе **«Разрешёния пользователя»** можно установить переключатель на опцию **«Пользователь не может изменить имя»**, но в этом нет крайней необходимости, так как подобная операция была выполнена на предыдущем шаге для всех сетей компьютеров организации.
5. Закрыть **«Редактор управления групповыми политиками»** и, при необходимости, обновить политики конфигурации компьютера, используя команду ***GPUpdate /Target:Computer /force /boot*** в командной строке.

Принудительное изменение профиля брандмауэра Windows в неопознанных сетях

В последние годы всё больше пользователь используют мобильные компьютеры. Используя свои мобильные компьютеры, пользователи могут подключаться к сети Интернет даже находясь в кафе, аэропортах или просто сидя на скамейке в парке. Именно

в таких случаях их компьютеры находятся под более существенным риском нападения злоумышленниками, нежели в корпоративной среде или у себя дома. Когда пользователь подключается к беспроводной сети, операционная система Windows автоматически определяет такую сеть как общедоступную. Для того чтобы настройки безопасности брандмауэра Windows применялись к компьютеру в зависимости от пользовательского места нахождения были разработаны профили брандмауэра. В том случае, если соединение проходит проверку подлинности на контроллере домена, то сеть классифицируется как тип **доменного** размещения сети. Если компьютер используется дома или в офисе – обычно применяется **домашняя** сеть с **частным** профилем брандмауэра. В местах общего пользования принято использовать **общий** профиль брандмауэра. Часто случается, что пользователи, находясь в общедоступных местах, пренебрегают этим средствам безопасности и для общедоступного профиля устанавливают частные профили брандмауэра.

Используя политики диспетчера списка сетей можно указать пользователю, какой профиль нужно использовать в случае неопознанных сетей, которые идентифицируются как «Общественная сеть». Для этого выполните следующие действия:

1. Открыть оснастку **«Редактор локальной групповой политикой»**.
2. В открывшемся окне, в дереве оснастки, перейти в узел **«Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики диспетчера списка сетей»** и открыть политику **«Неопознанные сети»**.
3. В диалоговом окне **«Свойства: Неопознанные сети»,** в группе **«Тип расположения»**, установив переключатель на нужную опцию, выбрать профиль брандмауэра, который будет сопоставлен с неопознанными сетями. В данном случае, устанавливается профиль **«Общий»**. В группе **«Разрешения пользователя»** можно установить переключатель на опцию **«Пользователь не может изменить расположение»** для того чтобы пользователь вручную не мог изменить сетевое расположение.
4. Закрыть **«Редактор локальной групповой политикой»** и, при необходимости, обновить политики конфигурации компьютера, используя команду ***GPUpdate /Target:Computer /force /boot*** в командной строке.

Политики открытого ключа. Файловая система EFS

Дополнительные функции шифрованной файловой системы (Encrypting File System, EFS) обеспечили дополнительную гибкость для корпоративных пользователей при развертывании решений безопасности, основанных на шифровании файлов с данными.

Любой злоумышленник, имеющий физический доступ к компьютеру, может загрузить на нем другую ОС, обойти защиту основной ОС и получить доступ к конфиденциальным данным. Шифрование конфиденциальных файлов средствами EFS обеспечивает дополнительную защиту. Данные зашифрованного файла останутся недоступными, даже если атакующий получит полный доступ к среде хранения данных компьютера.

Только полномочные пользователи и назначенные агенты восстановления данных в состоянии расшифровывать файлы. Пользователи с другими учётными записями, обладающие разрешениями для файла – даже разрешением на передачу прав владения (Take Ownership), не в состоянии открыть его. Администратору доступ к содержимому файла также закрыт, если только он не назначен агентом восстановления данных. При попытке несанкционированного доступа к зашифрованному файлу система откажет в доступе.

EFS и NTFS

Шифрованная файловая система (EFS) защищает конфиденциальные данные в файлах на томах NTFS. EFS – основная технология шифрования и расшифровки файлов на томах NTFS. Открывать файл и работать с ним может только пользователь, его зашифровавший. Это чрезвычайно важно для пользователей переносных компьютеров: даже если взломщик получит доступ к потерянному или украденному компьютеру, он не сможет открыть зашифрованные файлы. В Windows XP шифрованная файловая система также поддерживает автономные файлы и папки (Offline Files and Folders).

Зашифрованный файл останется недоступным для просмотра в исходном виде, даже если атакующий обойдет системную защиту, например, загрузив другую ОС. EFS обеспечивает устойчивое шифрование по стандартным алгоритмам и тесно интегрирована с NTFS. EFS в Windows XP предоставляет новые возможности совместного использования зашифрованных файлов или отключения агентов восстановления данных, а также облегчает управление посредством групповой политики и служебных программ командной строки.

Как работает EFS

EFS позволяет сохранить конфиденциальность информации на компьютере в условиях, когда люди, имеющие физический доступ к компьютеру, могут преднамеренно или неумышленно скомпрометировать её. EFS чрезвычайно удобна для обеспечения конфиденциальности данных на мобильных компьютерах или на компьютерах, на которых работают несколько пользователей, т. е. таких системах, которые могут подвергаться атакам, предусматривающим обход ограничений списков ACL.

В совместно используемой системе атакующий обычно получает несанкционированный доступ, загружая другую ОС. Злоумышленник также может захватить компьютер, вынуть жесткий диск, поместить его на другой компьютер и получить доступ к файлам. Однако если у него нет ключа расшифровки, зашифрованный средствами EFS файл будет выглядеть как бессмысленный набор символов.

Поскольку EFS тесно интегрирована с NTFS, шифрование и расшифровка выполняются незаметно («прозрачно») для пользователя. При открытии файла EFS автоматически расшифровывает его по мере чтения данных с диска, а при записи – шифрует данные при записи на диск.

В стандартной конфигурации EFS позволяет зашифровать файл прямо из Проводника Windows без какого-либо вмешательства администратора. С точки зрения пользователя шифрование файла или папки – это просто назначение ему определённого атрибута.

Что разрешается шифровать?

На томах NTFS атрибут шифрования разрешается назначать отдельным файлам и папкам с файлами (или подпапками). Хотя папку с атрибутом шифрования и называют «зашифрованной», сама по себе она не шифруется, и для установки атрибута пары ключей не требуется. При установленном атрибуте шифрования папки EFS автоматически шифрует:

- все новые файлы, создаваемые в папке;
- все незашифрованные файлы, скопированные или перемещённые в папку;
- все вложенные файлы и подпапки (по особому требованию);
- автономные файлы.

Политики ограниченного использования программ

Политики ограниченного использования программ предоставляют механизм идентификации программ и управления возможностями их выполнения. Существует два варианта установки правил ограничения:

- на всё программное обеспечение устанавливается ограничение на запуск и создаются исключения, то есть список программ, разрешенных к выполнению;
- разрешается запуск любых программ и создаётся список исключений, запрещающий запуск некоторых программ, доступ к программам определяется правами пользователя.

Для того чтобы выбрать один из вариантов как вариант по умолчанию, необходимо открыть пункт «Уровни безопасности» и выбрать нужный уровень. По умолчанию установлен уровень безопасности «Неограниченный», то есть запуск любых программ разрешен и необходимо создать исключения для запрета запуска определённых программ.

Политики ограниченного использования программ распространяются только на исполняемые файлы, чтобы посмотреть список таких файлов, перейдите в пункт «Назначенные типы файлов». В этот список можно добавить новый тип файлов, соответственно на такие файлы будут распространяться все установленные правила, или удалить какой-то тип, исключив такие файлы из правил политик.

Кроме того в пункте «Принудительный» существует возможность выбора, будут ли политики распространяться на файлы библиотек *.dll. Если политики будут распространяться и на файлы *.dll, то при установке уровня безопасности по умолчанию запрещающего выполнение программ, придется создавать дополнительные разрешения для каждой библиотеки которую использует программа, иначе программа будет работать некорректно.

С помощью политик ограниченного использования программ имеется возможность защищать компьютерное оборудование от программ неизвестного происхождения посредством определения программ, разрешенных для запуска. В данной политике приложения могут быть определены с помощью правила для хеша, правила для сертификата, правила для пути и правила для зоны Интернета. Программное обеспечение может выполняться на двух уровнях: неограниченном и запрещённом.

Политики ограниченного использования программ регулируют использование неизвестных программ и программ, к которым нет доверия. В организациях используется набор хорошо известных и проверенных приложений. Администраторы и служба поддержки обучены для поддержки этих программ. Однако, при запуске пользователем других программ, они могут конфликтовать с установленным программным обеспечением, изменять важные данные настройки или, содержать вирусы или «троянские» программы для несанкционированного удалённого доступа.

При применении политик ограниченного использования программ идентификация программного обеспечения производится посредством следующих правил:

- Правило для сертификата;
- Правило для пути;

Правило для пути идентифицирует программы по пути к файлу. Например, если имеется компьютер с политикой запрета по умолчанию, имеется возможность, предоставить неограниченный доступ к указанной папке для каждого пользователя. Для данного типа правил могут быть использованы некоторые общие пути: %userprofile%, %windir%, %appdata%, %programfiles% и %temp%.

Поскольку данные правила определяются с использованием пути, при перемещении программы правило для пути применяться не будет.

- Правило для хеша;

Хеш представляет собой серию байтов фиксированной длины, однозначно идентифицирующую программу или файл. Хеш рассчитывается с помощью алгоритма хеширования. Политики ограниченного использования программ могут идентифицировать файлы по их хешу с помощью алгоритмов хеширования SHA-1 (Secure Hash Algorithm) и MD5 hash algorithm.

Например, имеется возможность создать правило для хеша и задать уровень безопасности «Не разрешено», чтобы запретить запуск определённого файла. Хеш переименованного или перемещённого в другую папку файла не изменяется. Однако при любом изменении файла значение хеша изменяется, позволяя обойти ограничения.

Политики ограниченного использования программ распознают только хеши, рассчитанные с помощью политик ограниченного использования программ.

- Правило для зоны Интернета;

  Правила для зоны влияют только на пакеты установщика Windows.

Правило для зоны идентифицирует программное обеспечение из зоны, указанной посредством Internet Explorer. Такими зонами являются Интернет, локальный компьютер, местная интрасеть, ограниченные узлы и надёжные сайты.

В политиках ограниченного использования программ используются следующие уровни безопасности:

- *«Неограниченный»*. Приложения запускается со всеми правами пользователя, вошедшего в систему.
- *«Не разрешено»*. Приложения не могут быть запущены.

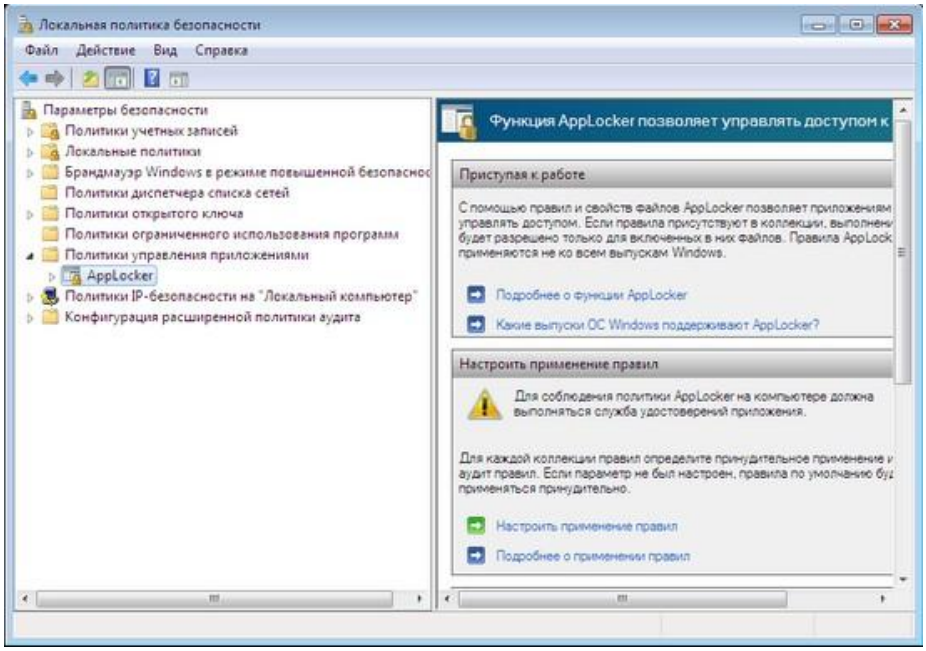
Политики управления приложениями

AppLocker – управление правами на запуск приложений.

AppLocker значительно упрощает контроль за действиями пользователей, которые касаются установки приложений, а также запуска файлов EXE, использования библиотек DLL, файлов инсталляторов MSI и MSP, а также сценариев. Основные отличия AppLocker от политик ограниченного использования программ:

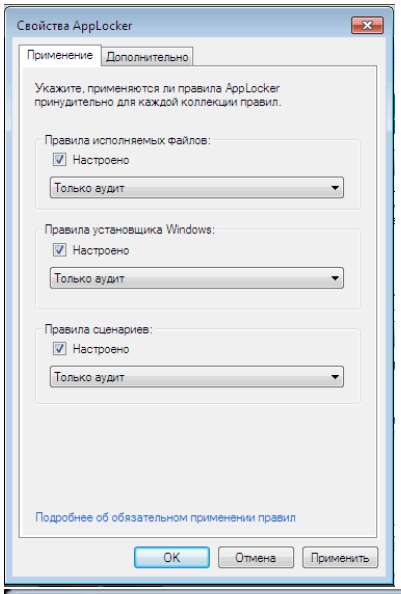
- применение правила к определённому пользователю или к группе, а не только ко всем пользователям;
- мастер автоматического создания правил;
- импорт и экспорт созданных правил;
- режим «Только аудит», в котором ведется аудит приложений, которые обрабатываются правилами, однако на самом деле правила не применяются;
- условие «Издатель», которое является расширенной версией условия «Сертификаты», существовавшего ранее;
- поддержка новой командной строки Windows Power Shell;
- коллекции правил для разных типов файлов, которые не зависят друг от друга.

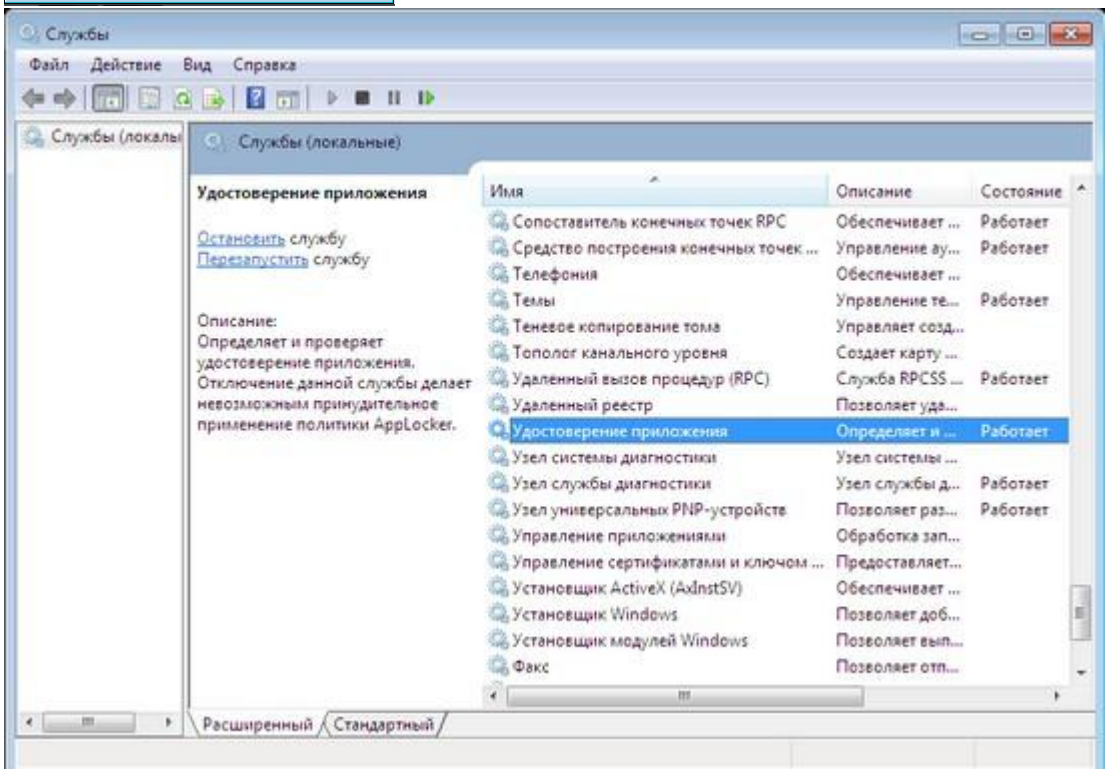
Для доступа к настройкам AppLocker необходимо перейти в раздел «Администрирование» (Administrative Tools) панели управления выбрать пункт «Локальная политика безопасности» (Local Security Policy), после чего раскрыть список «Политики управления приложениями» (Application Control Policies).



Одна из особенностей AppLocker состоит в том, что по умолчанию все правила, настроенные при помощи этого средства, применяются. Именно поэтому необходимо очень осторожно настраивать их, так как можно по неопытности заблокировать работу Windows. Во-первых, рекомендуется перед созданием правил перейти в окно их настройки, щёлкнув по ссылке «Настроить применение правил» (Configure Rule Enforcement), и для каждого типа правил (исполняемые файлы, установщик Windows и сценарии) выбрать вариант применения «Только аудит» (Audit Only). В этом случае правила с любыми настройками не смогут блокировать работу приложений или системы в целом, однако при помощи журнала событий администратор сможет просмотреть, как они применяются по отношению к файлам или приложениям. Если окажется, что правила блокируют приложения, к которым доступ должен быть разрешён, или, наоборот, не действуют на программы, к которым нужно ограничить доступ, правила можно будет отредактировать.

Второе решение, которое может помочь администраторам разобраться с новыми возможностями управления доступом, – создание и отладка правил на тестовом компьютере. AppLocker поддерживает импорт и экспорт правил, благодаря чему можно создать набор политик ограничений в безопасной среде, тщательно протестировать их работоспособность, после чего импортировать уже в рабочую среду.





Практическое занятие № 49-50

Тема: Механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов

Практическая часть:

Анализ трафика в сетях Ethernet

Цель работы:

• Получить практические навыки по работе с анализаторами сетевого трафика;

• На практике ознакомиться с различиями в принципах работы активного сетевого оборудования;

• Уяснить особенности взаимодействия сетевого и канального уровней на примере стека TCP/IP;

• Выяснить отличия форматов кадров Ethernet.

Необходимо:

• Компьютер под управлением MS Windows 2000/XP/2003 или Linux, подключенный к локальной сети;

• Пользователь с администраторскими правами; • Сетевое подключение по протоколу IP; • Доступ к глобальной сети Интернет.

• Программный пакет Wireshark.

Порядок выполнения работы:

1. Изучить назначение утилиты arp. Установить какие из широковещательных сообщений принадлежат протоколу ARP и для чего они предназначены.

2. Запустить программу Wireshark и получить сетевую статистику длительностью в 150 секунд.

Примечание: для увеличения интенсивности генерации кадров открыть любой информационный сайт в браузере.

3. Осуществить **визуализацию** полученных данных при помощи пункта меню построения графиков **Io Graphs**.

4. Используя сведения из пункта меню **Summary** определить длительность процесса анализа, количество захваченных пакетов, количество байтов, средний размер пакета, среднюю скорость передачи в Mbit/sec.

5. **Визуализировать** информационные потоки, образовавшиеся в результате работы при помощи пункта меню **Flow Graph.**

6. Выделить из общего числа **пакеты службы DNS.**

7. Определить **разницу во временах получения 1 и 2 пакетов** выделенных в предыдущем пункте.

8. Создать новый фильтр и захватить **5 Mb трафика**.

9. Создать **Display Filter** и выделить из общего числа пакеты по протоколам **TCP и UDP** предназначенные **для 80 порта**.

10. Создать **собственный фильтр**, захватывающий **30 пакетов** из трафика между используемым компьютером и сайтом **vkontakte.ru**.

11. Найти **широковещательные кадры и пакеты**. Изучить их **заголовки**. Выяснить их назначение. **Определить адреса**, на которые поступают данные кадры и пакеты **для канального и сетевого уровня.**

12. На основании собранной статистики определить, **к какому типу коммутационного оборудования** подключен используемый компьютер.

Примечание: в качестве коммутационного оборудования могут выступать **хаб**, **коммутатор** или **маршрутизатор**

В отчет:

1. Предоставить скриншоты результатов выполнения пунктов 3 и 5.

2. Сведения, определённые в пункте 4.

3. Текст фильтра, созданного в пункте 10.

Также в отчёте предоставить ответы на вопросы:

1. Какие **типы кадров Ethernet** бывают, в чем **их отличия**?

2. Какой тип кадров Ethernet используется в анализируемой сети? Почему именно он?

3. Как можно определить тип используемого коммутационного оборудования, используя сетевую статистику?

4. На какие адреса **сетевого** уровня осуществляются широковещательные рассылки?

5. На какой **канальный** адрес осуществляются широковещательные рассылки?

6. Для чего применяются **перехваченные** широковещательные рассылки?

7. Как с помощью утилиты **arp** просмотреть **arp-кэш** и как его **очистить**. В каких случаях может понадобиться последняя операция.

Практическая часть 2:

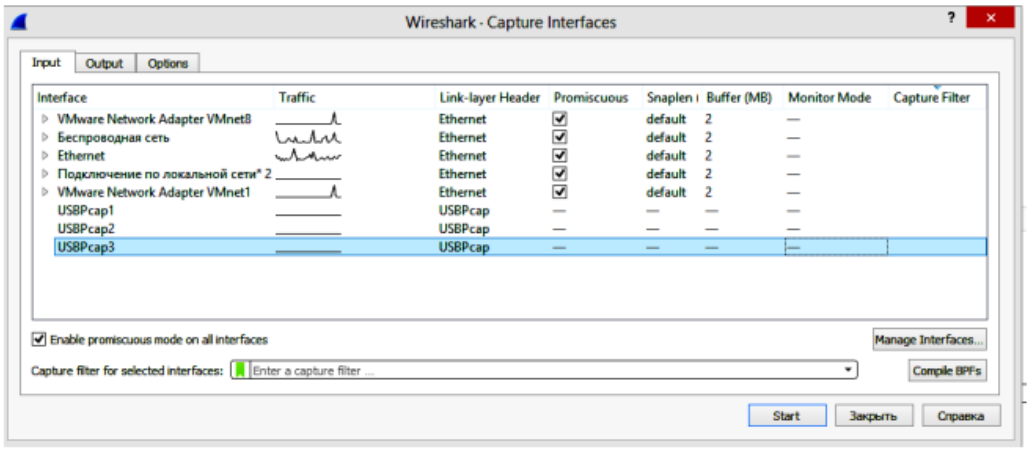
МОНИТОРИНГ СОСТОЯНИЯ ЭЛЕМЕНТОВ СЕТИ С ИСПОЛЬЗОВАНИЕМ АНАЛИЗАТОРОВ СЕТЕВОГО ТРАФИКА WIRESHARK

Установка программы и подготовка к захвату

1. Запустите Wireshark и разверните главное окно приложения на весь экран (для удобства работы)

2. Перед выполнением захвата сетевого трафика необходимо настроить параметры захвата или проконтролировать установленные значения некоторых из них так, чтобы собранная информация соответствовала решаемой задаче анализа трафика.

3. Выполните команду меню Capture ⇒ Options. В открывшемся диалоговом окне, как показано на рис.3.1. устанавливаются следующие параметры захвата кадров:



− Interface — сетевой адаптер;

Важно выбрать соответствующий сетевой адаптер, иначе запись кадров будет производиться из другого сегмента сети! В компьютере, имеющем всего один сетевой адаптер, 21 среди возможных сетевых интерфейсов часто присутствует контроллер удаленного доступа. − Buffer— размер буфера захвата (по умолчанию 2 Мб);

При малом размере буфера при его заполнении запись новых кадров будет производиться поверх записанных ранее. − Capture Filter — фильтр захвата; Фильтр захвата экономит объем буфера, отбрасывая «лишний мусор», однако увеличивает нагрузку на процессор, вследствие чего некоторые кадры могут быть потеряны.

Поэтому в некоторых случаях вместо фильтра записи предпочтительнее использовать фильтр отображения кадров в буфере, а запись производить без фильтрации. − Promiscuous mode — использование режима беспорядочного захвата.

5. Уберите маркер напротив опции «Promiscuous» для захвата только «своих» кадров (кадры с широковещательным адресом также будут захватываться). В таком режиме работы число захваченных пакетов будет существенно меньше, что облегчит выполнение заданий. 5. В Wireshark для запуска процесса захвата нажмите кнопку «Start». В командной строке выполните команду ping (в качестве параметра команды можно использовать IP-адрес любого хоста), как показано на рис.3.2. По завершении команды Ping остановите захват, нажав кнопку «Stop».

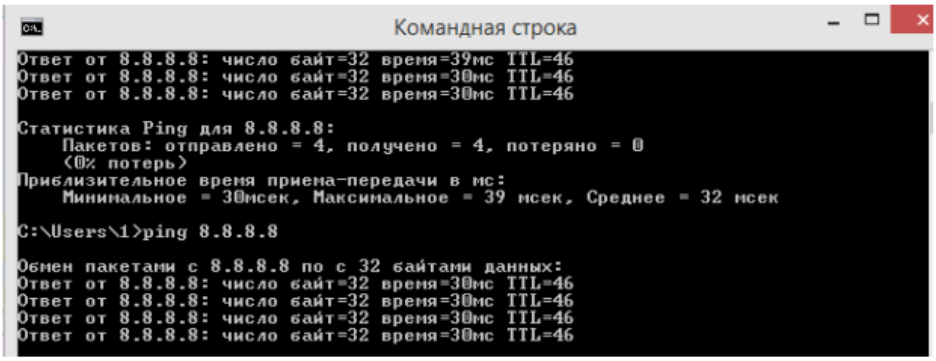


Рис.3.2. Выполнение команы ping

С помощью фильтра icmp можно оставить только те пакеты, которые передаются по данному протоколу, в данном случае отправляя пакеты с помощью команды ping используется именно этот протокол, как показано на рис. 3.3.

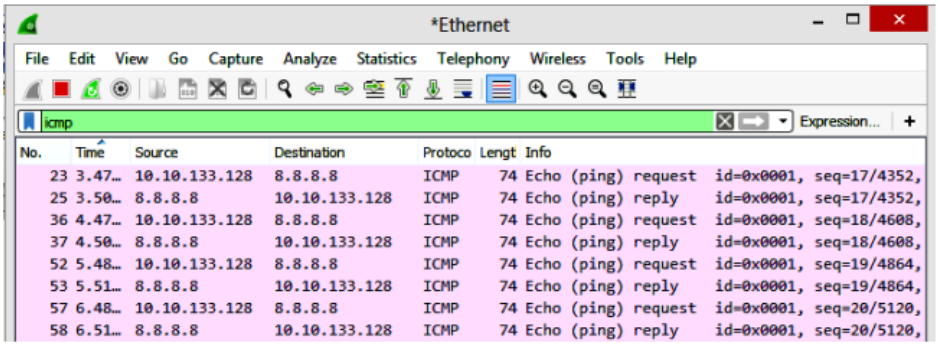


Рис 3.3. Результат перехвата трафика и применения фильтра для обнаружения ICMP сообщений

Анализ протоколов Ethernet и ARP

Отобразите в отдельных окнах пакеты запроса и ответа протокола ARP, как показано на рис.3.4, и ответьте на следующие вопросы:

– какое значение поля «тип протокола» в кадре Ethernet указывает на протокол ARP?

– по какому MAC-адресу отправлен запрос ARP?

– каким полем идентифицируются запрос и ответ ARP?

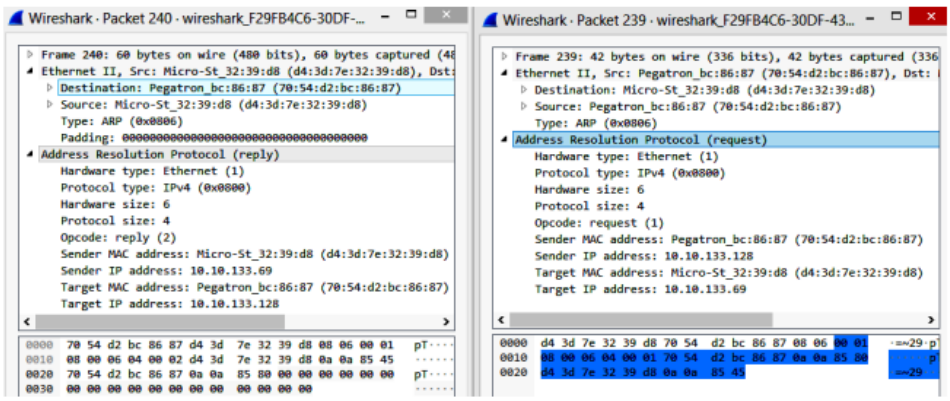


Рис. 3.4. Анализ ARP запрса и ответа

– в каких полях заголовка ARP передан запрос вашего узла?

– в каких полях заголовка ARP передан ответ вашему узлу?

Захватите сетевой трафик вашего узла при обращении к стартовой странице sfedu.ru, как показано на рис. 3.5 и ответьте на следующие вопросы:

– какие IP-адреса отображаются для узлов, участвующих в обмене по Протоколу IP?

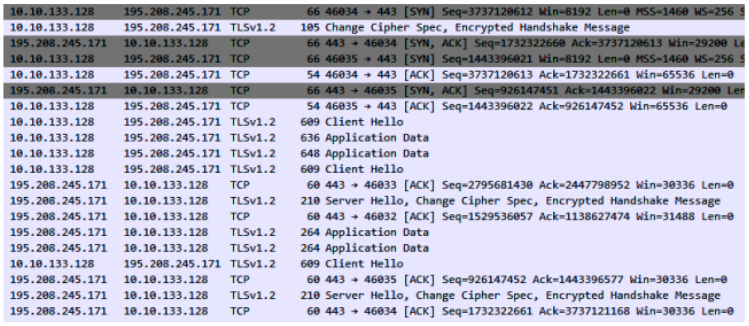


Рис. 3.5. Перехваченный трафик при обращению к серверу

Включите анализ заголовка IP, как показано на рисунке 3.6 и ответьте на следующие вопросы:

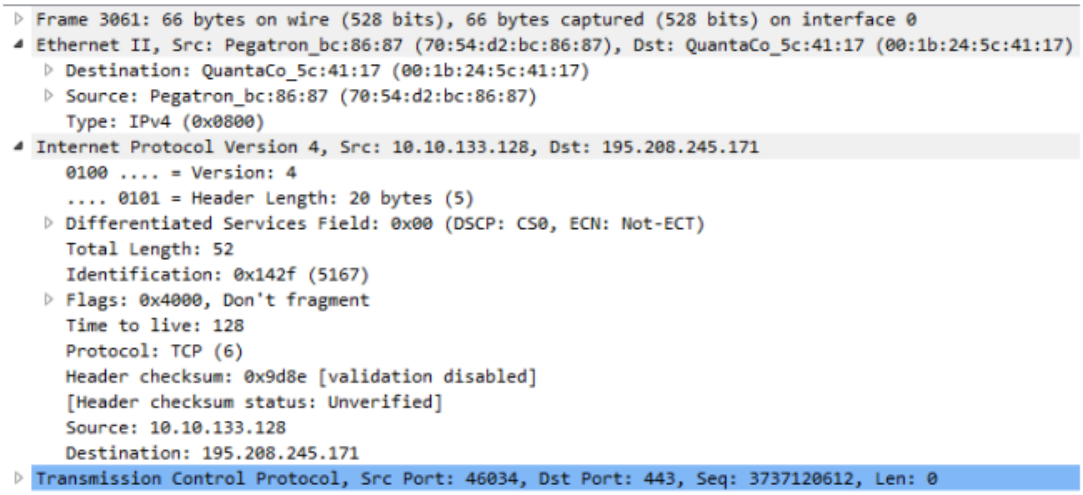


Рис. 3.6. Развернутый IP пакет

– какие IP-адреса отображаются для узлов, участвующих в обмене по протоколу IP?

– какие MAC-адреса имеют узлы, участвующие в обмене?

– какой IP-адрес имеет узел с MAC-адресом, присутствующим во всех кадрах с протоколом IP? Какова роль этого узла?

Проведите захват трафика команд ping и tracert при одинаковых значениях параметров l и n и проанализируйте различия в трафике этих команд.

– почему MAC адреса назначения и источника у всех кадров одинаковы и чьи это адреса?

– почему узлы присылают ICMP сообщение «type 11»?

– почему различные узлы присылают ICMP сообщение «type 11» на запрос к одному и тому же узлу?

– какова структура ICMP сообщения «type 11»?

– какие поля ICMP одинаковы, а какие различны в последних трех запросах?

С помощью фильтра отобразите только ICMPзапросы. Приведите выражение фильтрации и объясните, почему выражения 26 icmp.type == 8 и ip.src == X.X.X.X (где X.X.X.X —

IPадрес вашего узла) не приводят к желаемому результату. Каковы размеры кадров Ethernet, заголовков IP и сообщений ICMP, меняются ли они в процессе выполнения команды? Фрагментируются ли дейтаграммы, передаваемые узлом? Какие поля заголовка IP меняются, а какие остаются неизменными в каждом пакете трафика? 3.1.4. Анализ протокола TCP

Захватите сетевой трафик при обращении к стартовой странице сервера www.psct.ru, как показано на рис.3.7. Для отображения в буфере кадров с протоколом TCP примените соответствующее выражение фильтрации.

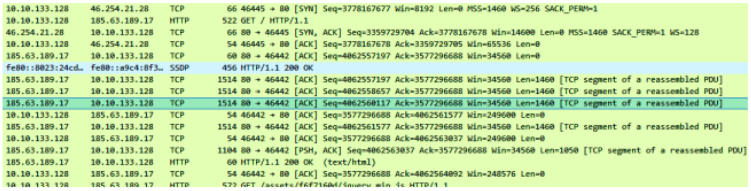


Рис. 3.7. Трафик перехваченный при обращении к сайту

Чем обращение к сайту www.psct.ru, отличается от обращения к сайту www.sfedu.ru? www.psct.ru

18. В перехваченном трафике определите начало TCP сессии. Какие порты используются клиентом и сервером? Какой начальный последовательный номер выбран клиентом? Какой бит флагов установлен и для чего он служит? Какие дополнительные опции TCP передаются клиентом в этом кадре?

19. Выберите первый сеанс и с помощью контекстного меню Apply as Filter ⇒ Selected ⇒ AB отобразите в буфере кадры, принадлежащие этому сеансу. 27

20. Определите, что передавалось в рамках захваченных вами сеансов TCP. В рамках захваченных сеансов TCP происходил обмен пакетами с данными с сайтом

21. Найдите фрагмент трафика, который соответствует закрытию TCP - сессии. Что такое трехстороннее рукопожатие, как можно обнаружить его в сетевом трафике? 3.2.

Контрольные вопросы

1. Что такое пассивные атаки, какие пассивные атаки вы знаете?
2. Перечислите основные компоненты сети, в чем их назначение?
3. Что такое сетевая карта интерфейса, для чего она используется?
4. Что такое коммутатор, чем он отличается от концентратора?
5. Какие внутренние атаки на сеть вы знаете?
6. Что такое маршрутизатор, чем он отличается от коммутатора?
7. Благодаря чему возможно проведение анализа сетевого трафика?
8. В каких режимах может работать сетевая карта?
9. Что такое трехстороннее рукопожатие?
10. Для чего нужны сетевые порты?
11. Перечислите основные компоненты сетевого анализатора трафика?
12. Что происходит на стадии захвата трафика?
13. Из чего состоит пакет, передаваемый по сети?
14. Для чего нужен заголовок, что такое инкапсуляция?

Практическое занятие № 51

Тема: Детализированные отчеты о нарушениях

Теоретическая часть:

Типовые нарушения в деятельности по защиты информации

Типовые недостатки и нарушения в деятельности объектовой системы защиты информации:

- отсутствуют необходимые для организации работ нормативно-методические документы по защите информации;
- объекту защиты не присвоена категория по требованиям обеспечения безопасности информации и (или) категория объекта документально не подтверждена;
- структура и содержание «Руководства по защите информации…» не соответствует установленным требованиям;
- не проведена оценка разведдоступности объекта защиты;
- не создана ПДТК по защите государственной тайны;
- деятельность коллегиального органа не организована и (или) его деятельность не способствует эффективному решению задач в области защиты информации;
- отсутствуют документы, регламентирующие работу комиссии (приказы, планы, решения, отчеты);
- отсутствует экспертная комиссия по проведению анализа материалов, предназначенных для открытого опубликования;
- деятельность ЭК не организована и (или) ее деятельность не способствует эффективному решению задач направленных на нераспространение информации ограниченного доступа;
- назначение руководителя подразделения (штатного специалиста) по технической защите информации не согласовано с ФСТЭК России;
- отсутствует подразделение (штатный специалист) по технической защите информации;
- функции по защите информации возложены на нештатного специалиста;
- специалисты по ТЗИ не проходили дополнительной подготовки на специализированных курсах повышения квалификации и (или) их уровень подготовки является недостаточным;
- не разработано Положение о подразделении (специалисте) по технической защите информации или содержание данного документа не учитывает требования Типового положения о подразделении по защите информации;
- мероприятия по технической защите информации и контролю не спланированы;
- на объекте контроля отсутствуют документы, регламентирующие порядок приема иностранных граждан или их содержание (порядок приема) не соответствует требованиям руководящих документов;

Типовые недостатки и нарушения в общей организации работ на средствах вычислительной техники:

- отсутствует инструкция по обеспечению режима секретности при обработке секретной информации с использованием средств вычислительной техники или данная инструкция не соответствует Типовой инструкции;
- не проводился или нарушены сроки проведения периодического контроля эффективности принимаемых мер защиты;
- обработка информации ограниченного доступа на неаттестованных по требованиям безопасности информации СВТ либо обработка такой информации на АС с неполученным или истекшим аттестатом соответствия;
- администраторы безопасности информации, являясь также пользователями автоматизированной системы, продолжают обрабатывать информацию под учетной записью с правами администратора;

- администратором безопасности информации не проводится аудит событий электронных журналов комплекса СЗИ от НСД;
- настройки СЗИ от НСД не соответствующее установленным требованиям для класса защищенности АС.

Типовые недостатки и нарушения в организации работ по защите речевой информации:

- обсуждение сведений, составляющих государственную тайну, ведется в помещениях, не подвергавшихся аттестационным испытаниям;
- в выделенном помещении отсутствуют сертифицированные средства защиты информации или их применение является недостаточным;
- технические паспорта на выделенные помещения отсутствуют или при их разработке (ведении) допущены недостатки;
- на ВТСС отсутствуют заключения по результатам специальных исследований и (или) специальных проверок (для ВТСС импортного производства) или протоколы инструментального контроля;
- реальный состав оборудования и технических средств, а также их размещение не соответствуют данным технических паспортов на ВП;
- несоответствие запланированных организационных и технических мер защиты ВП установленным требованиям.

Задание:

Составить детализированный отчет о нарушениях.

Практическое занятие № 52

Тема: Классификация уровня угрозы инцидента

Практическая часть:

Разработка модели угроз защищаемого объекта

Цель. Построение модели угроз безопасности защищаемого объекта информатизации.

Задачи.

1) Определение перечня угроз безопасности объекта.

2) Анализ каналов утечки информации.

3) Построение модели угроз с учетом каналов утечки.

4) Разработка модели вероятного нарушителя.

Определение перечня угроз безопасности объекта

Угроза - потенциальная возможность совершения действий направленных на нарушение безопасности объекта.

Проявление угроз (фактор неопределенности):

– действие нарушителей;

– воздействие стихийных сил;

– сбои в работе средств СФЗ;

– воздействие субъективного фактора.

Исходными данными для проведения оценки и анализа служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых на объекте и условий расположения и эксплуатации объекта.

Для составления перечня угроз необходимо:

– определить перечень актуальных источников угроз;

– определить перечень актуальных уязвимостей;

– оценить взаимосвязь угроз, источников угроз и уязвимостей;

– определить перечень возможных атак на объект;

– описать возможные последствия реализации угроз.

Угрозы утечки информации по техническим каналам.

1) Угрозы утечки речевой (акустической) информации по техническим каналам.

2) Характеристика угроз перехвата видовой (графической) информации ограниченного доступа визуальнооптическими средствами.

3) Угрозы утечки информации ограниченного доступа по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Технический канал утечки информации- совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка информации- неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней и ее получения разведками.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Основные элементы описания угроз утечки информации по техническим каналам представлены на рисунке 3.1.

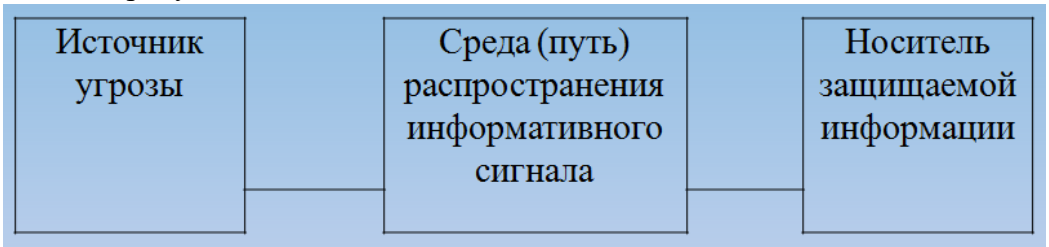


Рисунок 3.1 - Основные элементы угроз утечки информации

Носитель защищаемой информации- физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Задание 1.Составить перечень угроз для заданного объекта по образцу таблицы 3.1.

Таблица 3.1 - Перечень угроз

№ угрозы	Источник угрозы	Среда распространения	Носитель информации