

## **Описание модуля С: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием.

После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Для некоторых политик могут понадобиться дополнительные файлы, расположение которых можно узнать из карточки задания или у экспертов.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). Скриншоты необходимо сохранить в папке «Модуль 3».

Скриншоты необходимо называть в соответствии с номером задания и типом задания (Например Политика 2, Задание 1–1 и т. д.)

Задания на разработку политик можно выполнять в любом порядке.

Наиболее сложные политики находятся в конце.

Внимание!

Необходимо называть политики / объекты / категории / теги и прочее ТОЛЬКО в соответствии с номером и названием задания

Политики — Политика X, например «Политика 4».

Для комбинированных политик формат: Политика 4.1, 4.2 и т.д.

Объект защиты — Объект X, например «Объект 11».

Все политики «по умолчанию», находящиеся в консоли управления в процессе выполнения заданий должны быть отключены или удалены, так как могут помешать корректной оценке.

При разработке политик стоит учитывать, что все политики трафика могут передаваться как через веб-сообщения, так и через почтовые сообщения. В случае, если данный пункт не соблюден, то проверка заданий может быть невозможной.

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации.

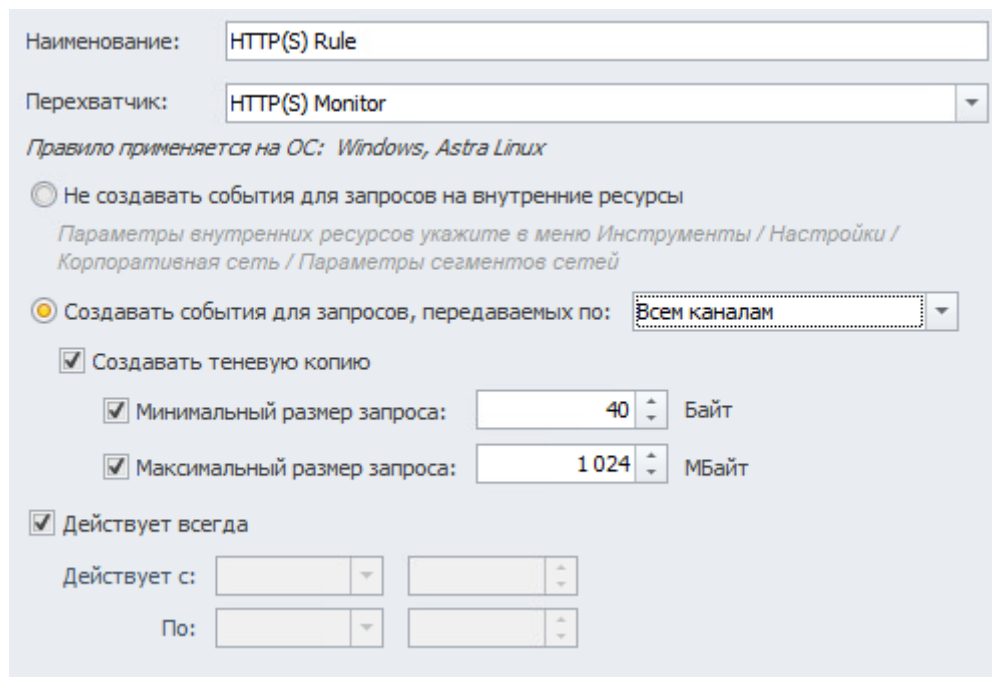
Список тегов для политик:

Политика 1, Политика 2, Политика 3, Политика 4, Политика 5, Политика 6, Политика 7, Политика 8, Политика 9, Политика 10, Политика 11, Политика 12

## Предисловие

Перед тем, как приступить к выполнению этого модуля, обязательно выполните следующие действия.

Перейдите к серверу IWDM, войдите в консоль управления Device Monitor. Перейдите к разделу «Политики» и создайте новое правило. В качестве наименования правила введите «HTTP(S) Rule», а в качестве перехватчика выберите HTTP(S) Monitor. Далее приведите правило к следующему виду.



The screenshot shows the configuration window for creating a new rule in the Device Monitor. The window has a light blue background and contains the following elements:

- Наименование:** A text input field containing "HTTP(S) Rule".
- Перехватчик:** A dropdown menu with "HTTP(S) Monitor" selected.
- Правило применяется на ОС:** A text label indicating "Windows, Astra Linux".
- Event Creation Options:**
  - ☐ Не создавать события для запросов на внутренние ресурсы. Below this is a note: "Параметры внутренних ресурсов укажите в меню Инструменты / Настройки / Корпоративная сеть / Параметры сегментов сетей".
  - ☒ Создавать события для запросов, передаваемых по: A dropdown menu with "Всем каналам" selected.
- Logging Options:**
  - ☒ Создавать теньюую копию.
  - ☒ Минимальный размер запроса: A numeric input field with "40" and a unit dropdown set to "Байт".
  - ☒ Максимальный размер запроса: A numeric input field with "1 024" and a unit dropdown set to "МБайт".
- Validity:**
  - ☒ Действует всегда.
  - Действует с:** Two empty date/time input fields.
  - По:** Two empty date/time input fields.

Рисунок 0 – Создание правила для прослушивания HTTP(S) трафика

Создайте аналогичное правило для второй политики.

## Задание 1

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты. Стоит учесть, что стандартные политики и объекты можно модифицировать под свои нужды.

### Задание 1: РЕШЕНИЕ

Для того чтобы удалить стандартные политики, перейдите к консоли управления IWTM, и перейдите в раздел «Политики». Затем поочередно: удалите каждую политику, нажимая на кнопку «Удалить» - крестик в левом верхнем углу каждой политики.

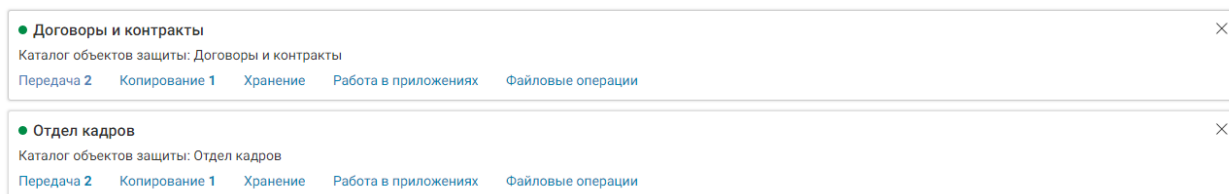



Рисунок 1 – Стандартные политики

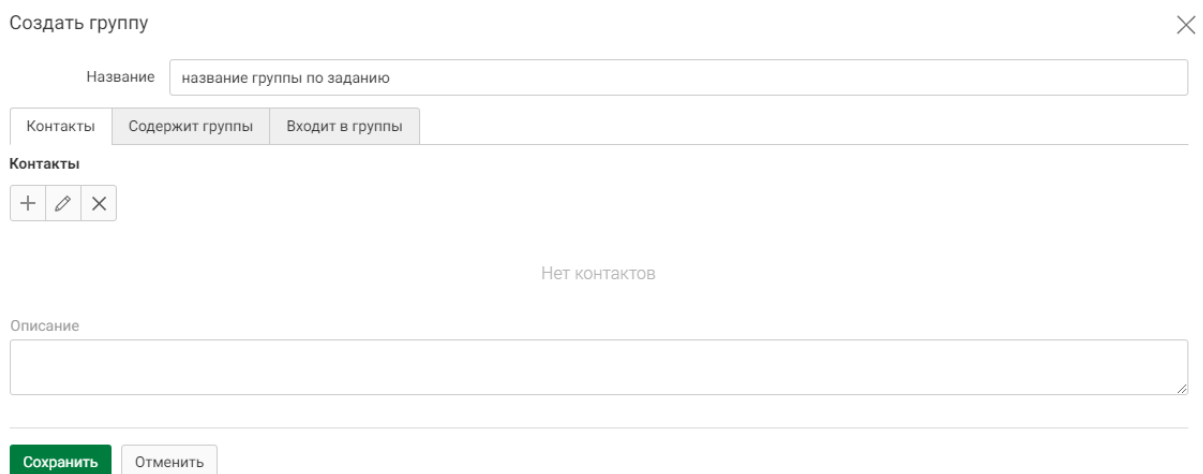
Теперь нужно отключить стандартные каталоги объектов защиты. Для этого, в консоли управления IWTM, перейдите ко вкладке «Объекты защиты». Слева вы увидите все каталоги объектов защиты, которые предустановлены на сервере мониторинга. Поочередно выбирайте каждый каталог, нажимайте на кнопку редактирования () и переведите Статус каждого из каталогов в отрицательное состояние.

## Задание 2

Создайте локальную группу пользователей «На испытательном сроке» в Traffic Monitor. Добавьте в нее трех любых пользователей.

### Задание 2: РЕШЕНИЕ

Для того, чтобы создать локальную группу пользователей в консоли Traffic Monitor перейдите ко вкладке «Персоны» и в левой части интерфейса выберите вкладку «Пользовательские группы», а затем нажмите кнопку «Создать группу» (плюсик). Назовите группу по заданию («Удалёнка», «На испытательном сроке» и т.п.).



The screenshot shows a 'Создать группу' (Create Group) dialog box. At the top, there is a title bar with a close button (X). Below it, a text input field labeled 'Название' (Name) contains the placeholder text 'название группы по заданию'. Underneath the input field are three tabs: 'Контакты' (Contacts), 'Содержит группы' (Contains groups), and 'Входит в группы' (Is a member of groups). The 'Контакты' tab is currently selected. Below the tabs, there is a section labeled 'Контакты' with three icons: a plus sign (+), a pencil (edit), and a cross (X). Below these icons, the text 'Нет контактов' (No contacts) is displayed. At the bottom of the dialog, there is a text input field labeled 'Описание' (Description). At the very bottom, there are two buttons: 'Сохранить' (Save) in green and 'Отменить' (Cancel) in white.

Рисунок 2 – Создание группы

Для добавления учетных записей из AD необходимо перейти в любую папку пользователей синхронизированную из AD и **ПЕРЕТАЩИТЕ** пользователя из родительской группы в созданную вами. Повторите с тем количеством пользователей, которое указано в задании.

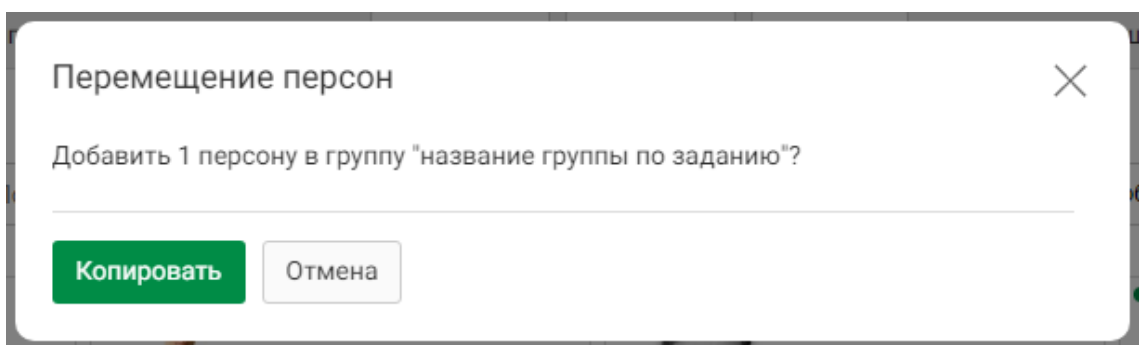


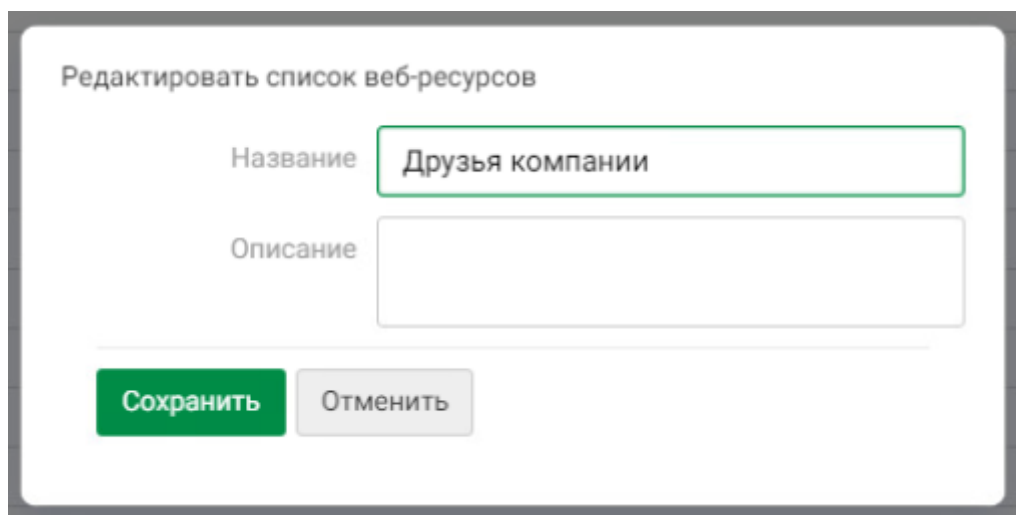
Рисунок 3 – Перемещение персон

### Задание 3

Создать список веб-ресурсов «Друзья компании». Добавить в список следующие сайты: demosystems.org, demo-software.ru, divine.lab.

### Задание 3: РЕШЕНИЕ

В этом задании может попадаться создание различных списков. Чтобы создать любой список перейдите ко вкладке «Списки». В данном примере, мы создадим список веб-ресурсов «Друзья Компании». Для создания списка веб-ресурсов во вкладке «Списки» перейдите к пункту «Веб-ресурсы». В левой верхней части интерфейса нажмите кнопку «Создать список веб-ресурсов», назовите его по заданию.



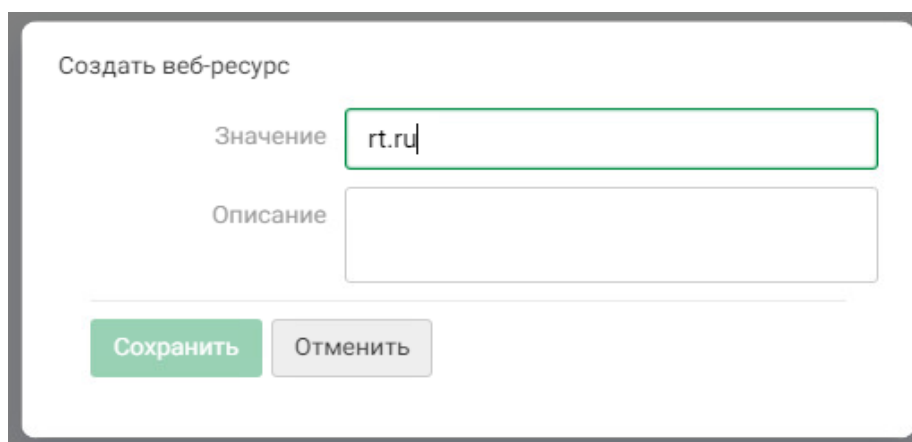
Редктировать список веб-ресурсов

Название

Описание

Рисунок 4 - Создание списка веб-ресурсов

Зайдите в каталог, нажмите кнопку «Добавить веб-ресурс» и введите одно из значений.



Создать веб-ресурс

Значение

Описание

Рисунок 5 — Добавление веб-ресурса

#### Задание 4

Для работы системы необходимо настроить периметр компании: Почтовый домен компании, список веб-ресурсов, группа персон «Удалёнка», исключить из перехвата почту генерального директора.

#### Задание 4: РЕШЕНИЕ

Для настройки периметра перейдите ко вкладке «Списки» и выберите «Периметры». Затем найдите периметр с названием «Компания», перейдите к настройкам и выставьте настройки по заданию.

В данном примере необходимо указать почтовый домен компании (имя домена, прим. demo.lab), список веб-ресурсов (который вы создавали в предыдущем задании), группу персон, указанную в задании. Также по заданию необходимо исключить почту генерального директора из перехвата.

##### Редактирование





Название	<input type="text" value="Компания"/>		
Список веб-ресурсов	<div><div>⋮</div>Друзья компании</div>	<div>+</div>	<div>×</div>
Почтовый домен	<div>@ demo.lab</div>	<div>×</div>	
Группа персон	<div><div>👤</div>Удалёнка</div>	<div>+</div>	<div>×</div>
<div><input type="checkbox"/> Использовать только рабочие контакты</div>			
<div>Добавить</div>			
Описание	<div>Персоны и компьютеры компании. Используется для контроля информации, передаваемой за периметр компании.</div>		
Создан: 21.02.2023 19:15		Изменен: 31.03.2023 14:44	
<div>Сохранить</div>		<div>Отменить</div>	

Рисунок 6 - Редактирование периметра

Чтобы исключить почту генерального директора из перехвата, необходимо перейти к периметру «Исключить из перехвата». Вероятнее всего,

почта генерального директора — kornilov@demo.lab. Если вы не уверены, найдите в оснастке «Пользователи и компьютеры Active Directory» запись о пользователе с описанием «Генеральный директор», там будет также указана его почта.

### Редактирование

Название	<input type="text" value="Исключить из перехвата"/>
Адрес электронной почты	<div> kornilov@demo.lab </div> <div>Добавить </div>
Описание	<div>Если включена политика 'Исключить из перехвата', то почтовые сообщения, отправленные входящими в данный периметр персонами,</div> 

Создан: 21.02.2023 19:15      Изменен: 21.02.2023 19:15

Сохранить

Отменить

Рисунок 7 — Исключение из перехвата



## **Политика 1**

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам, кроме отдела кадров отправлять документы, содержащие информацию о паспортных данных за пределы компании. Отдел кадров может отправлять файлы без ограничений.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 1

## **Политика 1: РЕШЕНИЕ**

Перед созданием политики, необходимо создать тэг. Для создания тэга, перейдите во вкладку «Списки» - «Теги». Нажмите кнопку «Создать тег» создайте тег для политики — назовите его по принципу «Политика X», где X — номер политики. Этот шаг будет необходимо повторять для каждой политики.

Также, перед созданием политики необходимо создать объект защищаемых данных. В данном задании необходимо ограничить передачу паспортные данные. Перейдите ко вкладке «Объекты защиты», создайте внутри новый каталог объектов защиты, назовите его по принципу «Политика X», где X — номер политики. Этот шаг также будет необходимо повторять для каждой политики.

После создания каталога, перейдите в него и нажмите кнопку «Создать...». Пройдите по каждой вкладке и впишите в поиск, то что необходимо защитить, в нашем примере - «Паспорт». В текстовых объектах выберите «номер подразделения», «паспорт гражданина РФ» и в графических объектах «паспорт гражданина РФ».

Ни в коем случае не отмечайте чекбокс «Создать объект защиты на каждый выбранный элемент, а затем нажмите «Создать». Далее откроется окно «Создание объекта защиты»: введите название в соответствии с

политикой «Политика 1». Во вкладке «Условия обнаружения» добавьте первое условие – выберите любой из объектов защиты, затем нажмите «Добавить условие» и вновь добавьте любой из объектов защиты.

Должно получиться примерно так:

The image shows a configuration interface for conditions. It consists of three identical-looking panels stacked vertically, each representing a condition. The panels are separated by the word 'или' (or).

- Condition 1:**
  - Title: **Условие**
  - Object: Паспорт гражданина РФ (Текстовый объект)
  - Threshold: Порог встречаемости (slider set to 1)
  - Button: Добавить элемент технологий
- Condition 2:**
  - Title: **Условие**
  - Object: Номер подразделения, выдавшего паспорт (Текстовый объект)
  - Threshold: Порог встречаемости (slider set to 1)
  - Button: Добавить элемент технологий
- Condition 3:**
  - Title: **Условие**
  - Object: Паспорт гражданина РФ (Графический объект)
  - Threshold: Порог встречаемости (slider set to 1)
  - Button: Добавить элемент технологий

Рисунок 0 – Условия обнаружения политики 1

Для создания политики в консоли IWTM перейдите во вкладку «Политики». Нажмите кнопку «Добавить политику...» - «Политика защиты данных». Назовите политику «Политика 1». В качестве защищаемых данных установите только что созданный объект защиты данных. Добавлять нужно именно конкретные объекты, а не каталоги объектов защиты.

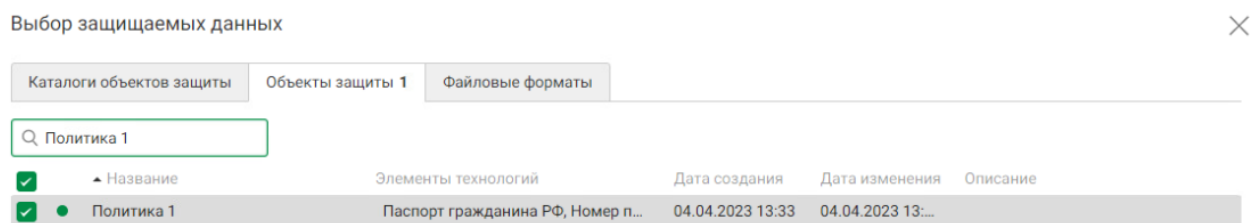


Рисунок 8 — выбор защищаемых данных

Нажмите сохранить, после чего еще раз нажмите сохранить в интерфейсе создания политики.

Теперь нажмите «Передача» и затем «Добавить правило».

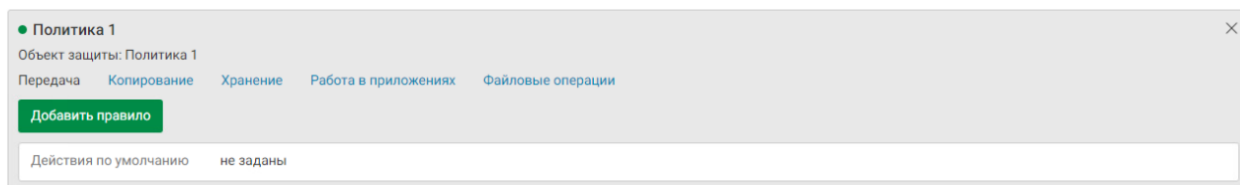


Рисунок 9 - созданная политика

Теперь конфигурируйте правило следующим образом:

- направление маршрута: в одну сторону,
- тип события: **ВСЕ**;
- компьютеры: **ПУСТО**;
- отправители: **=! «HR» (AD группа)**;
- получатели: **=! «Компания» (периметр)**;
- дни действия правила: **НЕ МЕНЯТЬ**;
- часы действия правила: **НЕ МЕНЯТЬ**.
- Действия при срабатывании правила:
- Отправить почтовое уведомление: **НЕ МЕНЯТЬ**;

- Назначить событию вердикт: **разрешить** (по заданию);
- Назначить событию уровень нарушения: **низкий** (по заданию);
- Назначить событию теги: «**Политика 1**»;
- Назначить отправителю статус: **НЕ МЕНЯТЬ**.

### Правило передачи

Направление маршрута	<input checked="" type="button" value="→ В одну сторону"/> <input type="button" value="⇄ В оба направления"/>	
Тип события	Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, ВКонтакте, Почта в Браузере, Почта на Клиенте	
Компьютеры	Начните вводить текст	<input data-bbox="1326 723 1374 779" type="button" value="+"/>
Отправители (?)	<input type="button" value="≠"/> <div> <input type="button" value="👤 HR"/> <input type="button" value="×"/> </div>	<input data-bbox="1326 813 1374 869" type="button" value="+"/>
Получатели (?)	<input type="button" value="="/> <div> <input type="button" value="⚙️ Компания"/> <input type="button" value="×"/> </div>	<input data-bbox="1326 902 1374 958" type="button" value="+"/>
Дни действия правила	Любой день недели	
Часы действия правила	0:00 <input type="button" value="🕒"/> -          0:00 <input type="button" value="🕒"/>	

### Действия при срабатывании правила

Отправить почтовое уведомление (?)	Начните вводить текст	<input data-bbox="1326 1352 1374 1408" type="button" value="+"/>
Назначить событию вердикт	<input checked="" type="button" value="✔️ Разрешить"/>	
Назначить событию уровень нарушения	<input checked="" type="button" value="● Низкий"/>	
Назначить событию теги	<input type="button" value="Политика 1"/> <input type="button" value="×"/>	<input data-bbox="1326 1621 1374 1677" type="button" value="+"/>
Назначить отправителю статус	Выберите статус	
Удалить событие	<input type="checkbox"/>	

Рисунок 9 - созданная политика

Теперь, правило нужно проверить на правильность срабатывания. Перейдите к любой из машин нарушителей (виртуальные машины с установленным агентом Device Monitor).

Откройте браузер, перейдите на сайт <http://dlptest.com>. На открывшемся сайте перейдите ко вкладке HTTP Post

## **Политика 2**

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании (документ «Анкета.docx»), контролируя любую внешнюю передачу документов, содержащих заполненные бланки, при этом пустые бланки контролировать не нужно.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 2

## **Политика 2: РЕШЕНИЕ**

Сделайте тег, и перейдите к созданию объекта защиты. В данном задании в качестве объекта защиты будет выступать эталонный документ «Анекта».

Для добавления эталонного документа необходимо перейти ко вкладке «Технологии», и перейти к разделу «Эталонные документы», и перейти к каталогу «Эталонные документы», после чего необходимо создать новый эталонный документ на основе всех типов данных». Выберите эталонный документ, а после его добавления перейдите к редактированию его настроек. Установите порог цитируемости данных в зависимости от задания. Нажмите сохранить и перейдите к созданию объекта защиты.

Редактировать ✕

Название

Анкета.docx

Полное имя файла

Анкета.docx

Формат файла

Документ Microsoft Word

---

Порог цитируемости текстовых данных

25%

Порог цитируемости бинарных данных

25%

Порог цитируемости определяет процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу

Рисунок 10 - настройки эталонного документа

Перейдите ко вкладке «Объекты защиты», создайте каталог «Политика 2», перейдите в него и добавьте внутрь созданный эталонный документ: не забудьте отметить галочку «создать объект защиты на каждый выбранный элемент».

Перейдите к созданию политики — в качестве защищаемых данных выберите только что созданный объект защиты данных:

- направление маршрута: в одну сторону,
- тип события: **ВСЕ**;
- компьютеры: **НЕ МЕНЯТЬ**;
- отправители: **НЕ МЕНЯТЬ**;
- получатели: **≠! «Компания»** (периметр);
- дни действия правила: **НЕ МЕНЯТЬ**;
- часы действия правила: **НЕ МЕНЯТЬ**.

Действия при срабатывании правила:

- Отправить почтовое уведомление: **НЕ МЕНЯТЬ**;
- Назначить событию вердикт: **Разрешить** (по заданию);
- Назначить событию уровень нарушения: **низкий** (по заданию);
- Назначить событию теги: **«Политика 2»**;
- Назначить отправителю статус: **НЕ МЕНЯТЬ**.

### Правило передачи

Направление маршрута	<div>→ В одну сторону</div> <div>⇌ В оба направления</div>		
Тип события	Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, ВКонтакте, Почта в Браузере, Почта на Клиенте		
Компьютеры	Начните вводить текст		+
Отправители ?	=	Начните вводить текст	+
Получатели ?	≠	Компания ×	+
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	Политика 2 ×	+
Назначить отправителю статус	Выберите статус	▼

Рисунок 11 - настройки второй политики



### Политика 3

В связи с введением оплаты с помощью кредитных карт, необходимо запрещать передачу как текстовых, так и графических данных о кредитных картах за пределы компании для всех сотрудников, кроме отдела договоров (accounting). Политика может быть настроена с использованием стандартных технологий и объектов.

Вердикт: заблокировать

Уровень нарушения: средний

Тег: Политика 3

### Политика 3: РЕШЕНИЕ

Здесь не нужно создавать дополнительные технологии, как в предыдущей политике. Создайте тег и переходите к созданию объекта защиты данных, создайте каталог, а внутрь добавьте объекты защиты.

Добавьте в каталог графические (кредитная карта) и текстовые данные (номер кредитной карты, номер кредитной карты (16 цифр)). Не забудьте о галочке «создать объект защиты на каждый выбранный элемент».

Перейдите к созданию политики:

- защищаемые данные: только что созданные вами данные - номер кредитной карты, номер кредитной карты (16 цифр), кредитная карта;
  - направление маршрута: в одну сторону,
  - тип события: **ВСЕ**;
  - компьютеры: **НЕ МЕНЯТЬ**;
  - отправители: **=! «Accounting»** (группа FD);
  - получатели: **=! «Компания»** (периметр);
  - дни действия правила: **НЕ МЕНЯТЬ**;
  - часы действия правила: **НЕ МЕНЯТЬ**.
  -

- Действия при срабатывании правила:
- Отправить почтовое уведомление: **НЕ МЕНЯТЬ**;
- Назначить событию вердикт: **заблокировать** (по заданию);
- Назначить событию уровень нарушения: **Средний** (по заданию);
- Назначить событию теги: **«Политика 3»**;
- Назначить отправителю статус: **НЕ МЕНЯТЬ**.

### Правило передачи

Направление маршрута	<input checked="" type="radio"/> В одну сторону <input type="radio"/> В оба направления	
Тип события	Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, ВКонтакте, Почта в Браузере, Почта на Клиенте	
Компьютеры	Начните вводить текст	+
Отправители ?	<input type="text" value="≠"/> <div>Accounting ×</div>	+
Получатели ?	<input type="text" value="≠"/> <div>Компания ×</div>	+
Дни действия правила	Любой день недели	
Часы действия правила	<input type="text" value="0:00"/> <input type="text" value="0:00"/>	

### Действия при срабатывании правила

Отправить почтовое уведомление ?	Начните вводить текст	+
Назначить событию вердикт	<input checked="" type="radio"/> Заблокировать	
Назначить событию уровень нарушения	<input checked="" type="radio"/> Средний	
Назначить событию теги	<input type="text" value="Политика 3"/>	+
Назначить отправителю статус	Выберите статус	

Рисунок 12 — Создание третьей политики

## Политика 4

Необходимо отслеживать любые документы, передающиеся за пределы компании и содержащие печать компании всем сотрудникам, кроме отдела продаж (Sales) и директора компании. Они могут обмениваться документами внутри и за пределами компании без контроля.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 4

### **Политика 4: РЕШЕНИЕ**

Здесь необходимо создать собственный элемент технологии — печать компании. Перейдите ко вкладке «Технологии» - «Печати», создайте каталог, затем нажмите кнопку «Добавить печать» и выберите файл с печатью.

## Правило передачи

Направление маршрута	<div>→ В одну сторону</div> <div>⇌ В оба направления</div>	
Тип события	Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, ВКонтакте, Почта в Браузере, Почта на Клиенте	
Компьютеры	<div>Начните вводить текст</div>	<div>+</div>
Отправители (?)	<div>=</div> <div>Начните вводить текст</div>	<div>+</div>
Получатели (?)	<div>≠</div> <div><div><div>👤 Sales</div><div>×</div></div><div><div>👤 Kornilov V. Fedosej</div><div>×</div></div></div>	<div>+</div>
Дни действия правила	Любой день недели	
Часы действия правила	<div>0:00</div> <div>🕒</div>	<div>-</div> <div>0:00</div> <div>🕒</div>

## Действия при срабатывании правила

Отправить почтовое уведомление (?)	<div>Начните вводить текст</div>	<div>+</div>
Назначить событию вердикт	<div>✔ Разрешить</div>	
Назначить событию уровень нарушения	<div>● Низкий</div>	
Назначить событию теги	<div>Начните вводить текст</div>	<div>+</div>
Назначить отправителю статус	<div>Выберите статус</div>	
Удалить событие	<div><input type="checkbox"/></div>	