ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Business Email Protection»

Руководство администратора

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Определение
Алерт	Предупреждение об опасности. «Немедленное» оповещение о том, что информационная система и сеть подвергаются атаке или находятся в опасности вследствие аварии, сбоя или человеческой ошибки.
ОС	Операционная Система
ПО	F6 Business Email Protection, BEP
iDRAC	Integrated Dell Remote Access Controller. Проприетарный контроллер удалённого доступа, мониторинга и управления.
iLO	Проприетарный интерфейс Integrated Lights-Out. механизм управления серверами в условиях отсутствия физического доступа к ним.
IPv4	Internet Protocol version 4
KVM	Kernel-based Virtual Machine. Программное решение, обеспечивающее виртуализацию в среде Linux на платформе x86, которая поддерживает аппаратную виртуализацию.
MDP	Модуль F6 Malware Detonation Platform
MXDR	Программный комплекс Managed Extended Detection and Response (Managed XDR)
NTA	Модуль F6 Network Traffic Analysis
SaaS	Software as a Service. Модель обслуживания, при которой программное обеспечение размещено в облачной инфраструктуре.
SOC	Security Operation Center. Центр мониторинга киберугроз и предотвращения инцидентов кибербезопасности.
SSH	Secure Shell. Сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений.

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ описывает процесс установки экземпляра программного обеспечения «F6 Business Email Protection» (далее – ПО, BEP).

Инструкция по установке распространяется только на вариант распространения ПО в формате On-prem. Для Cloud (SaaS) версии установка ПО не требуется.

В случае возникновения проблем с разворачиванием ПО необходимо обратиться в техническую поддержку

1.2 Назначение ПО

«F6 Business Email Protection» - это модуль системы MXDR (Managed XDR) который специализируется на анализе и мониторинге электронной почты для выявления киберугроз. Этот модуль сканирует входящие письма для обнаружения фишинга, спама и других видов угроз, направленных на компрометацию пользователей. ПО фокусируется на проверке содержимого писем и выявлении потенциальных угроз. В качестве платформы детонации используется модуль Malware Detonation Platform (MDP). В случае обнаружения угроз модуль формирует отчеты и отправляет уведомления, обеспечивая оперативное реагирование специалистов по кибербезопасности.

2 ТРЕБОВАНИЯ К СИСТЕМЕ

ПО может быть установлено либо на физический сервер, либо на виртуальную машину.

2.1 Минимальные технические требования для физического сервера

Ниже приведены минимальные технические требования к серверу в зависимости от типа ПО. Основным параметром выбора минимального оборудования является сервер NTA Prevent, в связке с которым работает BEP в независимости от типа поставляемой лицензии (BEP Standard, BEP Pro, BEP Enterprise)

Параметр	1000	5000	10 000
Процессор(ы)	Intel Xeon Gold 5315Y 3.2GHz, 8C/16T, 11.2 GT/s, 12MB Cache, Turbo 3.6GHz, HT (140W) DDR4-2933	Intel Xeon Gold 6336Y 2.4GHz, 24C/48T, 11.2GT/s, 36M CacheTurbo 3,6GHz HT (185W) DDR4-3200	Intel Xeon Gold 6348 2.6GHz, 28C/56T, 11.2GT/s, 42 M Cache Turbo 3,5GHz, HT (235W) DDR4-3200
Объем хранилища	2 x 480GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS SSD RAID1	2 x 960 GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1	2 x 960GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1
Интерфейс управления	1 Ethernet	1 Ethernet	1 Ethernet
Объем оперативной памяти	64 GB	64 GB	128 GB
Интерфейс анализатора сетевого трафика (NTA)	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter

2.2 Минимальные технические требования для виртуальной машины

Ниже приведены минимальные технические требования к конфигурации оборудования виртуальной машины.

Параметр	1000	5000	10 000
Виртуальный процессор	16	40	56
Объем хранилища	480 GB SSD, Random write 44500 IOPS	960 GB SSD, Random write 44500 IOPS	960 GB SSD, Random write 44500 IOPS
Объем оперативной памяти	64 GB	64 GB	128 GB

Параметр	1000	5000	10 000
Интерфейс анализатора сетевого трафика (NTA)	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter

2.3 Требования к программному обеспечению

Требования к программному обеспечению не предъявляются, так как ПО является частью самостоятельных операционных систем, реализованных на базе Linux с версией ядра Linux 5.11.16-arch1-1 и Linux 5.15.14-1-lts. Программное обеспечение устанавливается совместно с модулями «F6 XDR» (MXDR Console), «F6 NTA» (Network Traffic Analysis) и «F6 MDP» (Malware Detonation Platform). Работоспособность ПО достигается путем интеграционных настроек вышеупомянутых модулей между собой.

3 УСТАНОВКА ТЕСТОВОЙ ВЕРСИИ ПО

«F6 Business Email Protection» не функционирует как автономное программное обеспечение, а интегрируется в состав модулей NTA (Prevent) и XDR (MXDR Console). Установка ПО осуществляется одновременно с установкой этих модулей. Функциональность ПО может быть расширена при подключении ПО, который представляет собой платформу детонации файлов для углубленного анализа угроз.

4 Сценарии проверки работоспособности ПО

4.1 Локальное размещение «F6 Business Email Protection» (On-prem)

Для корректного проведения тестирования, необходимо выполнение пунктов по проверке работоспособности продуктов XDR (MXDR Console) и MDP, а также наличие корректной интеграции NTA с MDP.

1. Настройка инфраструктуру на стороне заказчика:

– для интеграции по протоколу SMTP (копия писем): сетевая доступность между NTA и почтовым сервером, отправка копии почтового потока на 25 порт NTA;

– для интеграции по POP3/IMAP: почтовый ящик, к которому будет подключаться NTA и забирать копию писем, сетевая доступность между NTA и почтовым сервером;

– для интеграции в режиме MTA: сетевая доступность между NTA и почтовым сервером, настройка отправки почтового потока на 25 порт NTA, настройка получения проанализированного почтового потока от NTA.

2. Настройка на стороне сенсора:

– для интеграции по протоколу SMTP (копия писем): перейти в раздел ***Настройки*** → ***Модули*** → ***NTA*** → ***Основные настройки*** → ***Почта*** → ***Почтовый сервер*** и включить эту опцию. Настройку режима работы модуля выставить в значение “*Прием копии писем*”.

– для интеграции по POP3/IMAP: перейти в раздел ***Настройки*** → ***Модули*** → ***NTA*** → ***Основные настройки*** → ***Почта*** → ***Почтовый клиент***.

– для интеграции в режиме MTA: перейти в раздел ***Настройки*** → ***Модули*** → ***NTA*** → ***Основные настройки*** → ***Почта*** → ***Почтовый сервер***. Настройку режима работы модуля выставить в значение “*MTA*”. Далее проверить наличие почтовых маршрутов для дальнейшей отправки почты и включить режим блокировки почты.

3. Проверить в разделе ***Настройки*** → ***Модули*** → ***NTA*** → ***Основные настройки*** → ***Почта*** → ***Синхронизация*** с MXDR Console в положение “*Включено*”.

4. Далее на тестовый почтовый адрес отправить письмо. Наличие записи об этом письме в разделе ***Расследования*** → ***Письма*** свидетельствует о поступлении почты на анализ.

5. Далее на выбранный почтовый ящик необходимо запустить синтетический тест (отправить ВПО).

6. По завершению теста и завершению анализа всех отправленных писем, должны быть сформированы алерты о вредоносных письмах в разделе ***Атаки*** → ***Алерты***, а также должны быть доступны отчеты MDP по файлам во вложениях/ссылкам. При интеграции в режиме MTA вредоносные письма, не находящиеся в статусе “ретро-анализ” должны быть заблокированы и не доставлены на указанный почтовый ящик.

4.2 Облачное размещение «F6 Business Email Protection»

Для корректного проведения тестирования, необходимо выполнение пунктов по проверке работоспособности продуктов XDR (MXDR Console).

1. Проверка подключения необходимой лицензии: перейти в раздел Настройки → Модули → Business Email Protection → Индикатор слева горит зеленым ИЛИ в Настройках присутствует пункт “Облачная Почта”.

2. Настройка модуля:

– В настройках модуля, в разделе “*Домены и маршруты*” в пункт “*Почтовые домены*” добавлены защищаемые домены и находятся в статусе “*Подтверждено*”;

– В настройках модуля, в разделе “*Домены и маршруты*” в пункт “*Почтовые маршруты*” добавлены маршруты доставки почтовых сообщений после проведения проверки;

– Если модуль используется в качестве второго почтового релея, в настройках модуля, в разделе “*Домены и маршруты*” в пункт “*Входящий шлюз*” внесен IP-адрес отправляющего контент первого шлюза.

3. Настройка инфраструктуры на стороне заказчика:

– IP-адреса BEP внесены в список доверенных отправителей в настройках почтового шлюза;

– MX-записи BEP внесены в MX-записи защищаемых доменов;

– При интеграции модуля внутри инфраструктуры в качестве второго почтового релея необходимо убедиться, что в настройках первого почтового релея добавлен маршрут об отправке почты на IP-адреса модуля BEP.

4. Послать тестовое письмо на защищаемый домен с внешнего источника. Чтобы увидеть результат, необходимо перейти в раздел ***Расследование*** → ***Проверенные письма*** и отфильтровать почту по отправителю письма, используя ключевое выражение mail_from.

5. Настройка белого списка: в раздел ***Настройки → Модули → Business Email Protection → Основные настройки → Политика и обнаружение → Белый список антиспама*** ИЛИ в ***Настройки → Облачная почта → Политика и обнаружение → Белый список антиспама*** внесены доверенные домены отправителей, а также другие домены, относящиеся к инфраструктуре заказчика.

6. Настройка модуля анализа нежелательных писем: перейти в ***раздел Настройки → Модули → Business Email Protection → Основные настройки → Политика и обнаружение → Выявление нежелательных писем*** ИЛИ в ***Настройки → Облачная почта → Политика и обнаружение → Выявление нежелательных писем*** и проверить, он сконфигурирован следующим образом:

- Включен Статический классификатор,
- Включен Эвристический классификатор,
- Действие → Карантин.

7. Отправить тестовое нежелательное письмо, предоставленное разработчиками АО «БУДУЩЕЕ», на защищаемый почтовый ящик. Чтобы увидеть результат, необходимо перейти в раздел ***Расследование → Проверенные письма → Нежелательные*** и отфильтровать почту по отправителю письма, используя ключевое выражение mail_from.

8. Настройка модуля детонации файлов (при наличии модуля детонации): перейти в раздел ***Настройки → Модули → Business Email Protection → Основные настройки → Политика и обнаружение → Детонация файлов*** ИЛИ в ***Настройки → Облачная почта → Политика и обнаружение → Детонация файлов*** и проверить, что данный модуль включен и настроен следующим образом:

- Действие – Карантин + Уведомление получателя,
- Язык в виртуальных машинах – Соответствует локализации заказчика.

Отключить для проведения теста модуля детонации файлов модуль выявления нежелательных писем. Далее отправить тестовое письмо на защищаемый домен с внешнего источника. В письме должна содержаться вредоносная нагрузка (будет предоставлена сотрудниками АО «БУДУЩЕЕ». Самостоятельно можно пройти бесплатное тестирование Trebuchet). Чтобы увидеть результат, необходимо перейти в раздел ***Расследование → Проверенные письма → Вредоносные*** и отфильтровать почту по отправителю письма, используя ключевое выражение mail_from.

5 Администрирование Business Email Protection

5.1 Домены и маршруты

5.1.1 Глобальные настройки

Все настройки в данном разделе относятся только к устройствам с **Cloud Business Email Protection.**

5.1.1.1 MX-записи серверов Business Email Protection

Актуальные MX-записи.

- mx1.atmosphere.facct.ru
- mx2.atmosphere.facct.ru

5.1.1.2 IP-адреса серверов Business Email Protection

- Для mx1.atmosphere.facct.ru: - `82.202.245.76` - `82.202.245.77`
- Для mx2.atmosphere.facct.ru: - `94.26.244.116` - `94.26.244.117`

Рекомендуется выставлять MX-серверы **BEP** в качестве приоритетных, а ранее использованные MX-серверы оставлять с более низким приоритетом. Если все работает корректно, вы можете удалить старые MX-записи и разрешить подключение **только** с адресов **BEP**, чтобы не оставить злоумышленникам путей обхода.

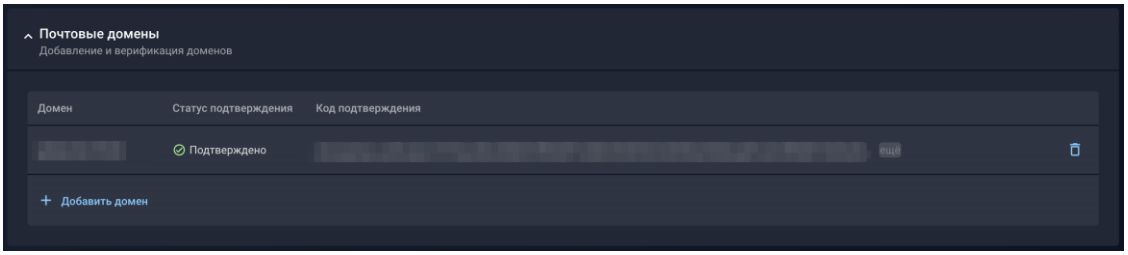
*Примечание: все MX-серверы **Business Email Protection** должны иметь равный приоритет.*

5.1.2 Почтовые домены

Использование данного раздела позволяет добавлять и верифицировать почтовые домены. Для защиты почтовых входящих сообщений необходимо:

1. Добавить домен в список.
2. Добавить сформированный код подтверждения в `TXT` запись домена. Данная операция осуществляется в административной панели регистратора домена.
3. Дождаться верификации домена модулем **Business Email Protection**.

Необходимо использовать кнопку **Обновить** справа от домена, чтобы получить актуальную информацию о ходе верификации домена.



Статусы домена:

- **Подтверждено** – Подтверждённый статус домена. Код подтверждения добавлен в TXT запись домена.
- **Не подтверждено** – Код подтверждения не был добавлен в TXT запись домена. Возможно, DNS еще не обновился и необходимо повторить попытку позднее.

5.1.3 Почтовые маршруты

Необходимые настройки:

- **Домены получателя** – Обслуживаемые почтовые домены и/или поддомены клиента.
- **Подтв. RCPT TO** – При включении **BEP** проверяет наличие получателя в MX серверах клиента. (Открывается встречная SMTP сессия на требуемое имя. По ответу от MX определяется наличие или отсутствие данного получателя у клиента).

*Примечание: для данной проверки используется SMTP-команда **VRFY**. Не рекомендуется включать эту настройку, если сервер-получатель данную команду не поддерживает.*

- **MX адрес** – Адрес почтового сервера клиента. Он же адрес следующего хопа в цепочке проверки почтовых сообщений.
- **Порт** – Порт на MX сервере клиента для отправки проверенных сообщений.
- **TLS** – Использование TLS для формирования всех коммуникаций с отправителями и получателями почтовых сообщений.
- **Приоритет** – Приоритетность опроса серверов клиента. Приоритет определяет в каком порядке опрашиваются сервера при недоступности некоторых серверов.
- **Вес** – Балансировка нагрузки на сервера клиента. Вес отвечает за балансировку в пределах одного приоритета.

5.1.4 Режимы использования TLS

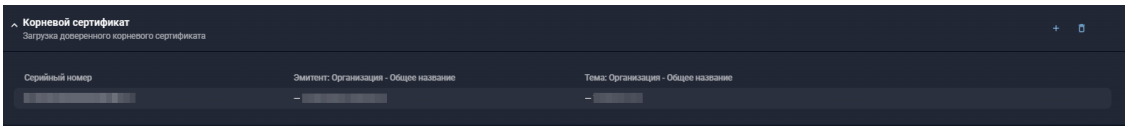
При редактировании определенного домена можно выбрать один из следующих режимов использования TLS:

- **No TLS** — Не использовать шифрование.

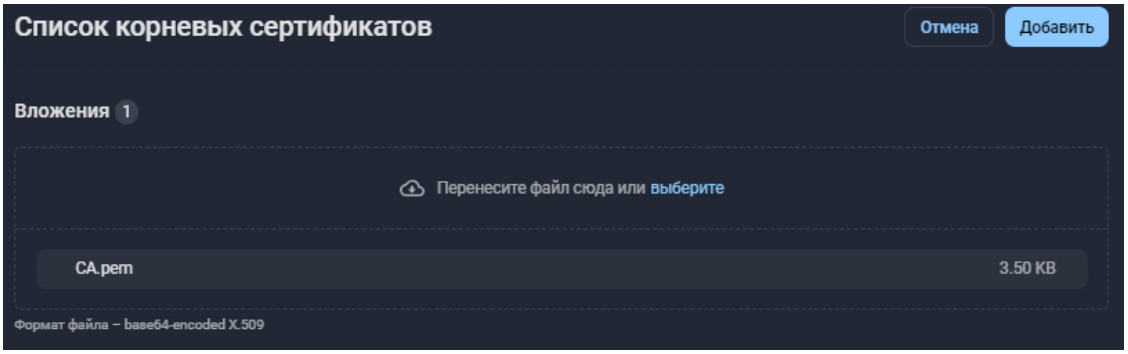
- **No validation** — Использовать шифрование и доверять любому сертификату.
- **Secured** — Использовать шифрование с валидацией сертификата.

5.1.5 Корневой сертификат

Использование данного раздела позволяет загрузить доверенный корневой сертификат.



Чтобы добавить корневой сертификат необходимо нажать кнопку plus-icon или **Добавить значения**, если сертификат добавляется впервые. Откроется сайдбар с областью для добавления корневого сертификата.

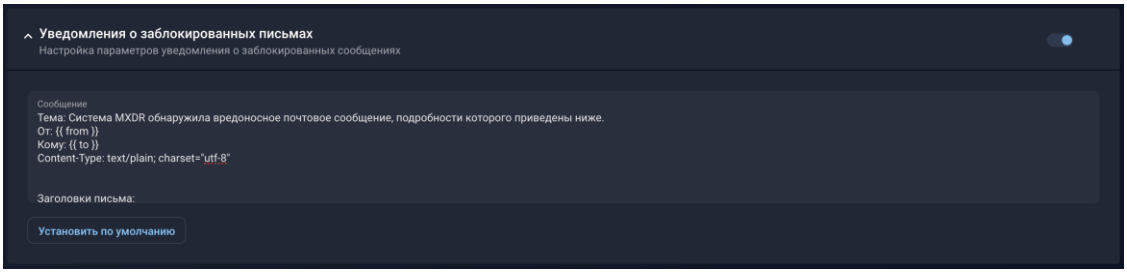


В область необходимо перетащить файл корневого сертификата (либо выбрать файл через проводник (explorer), используя кнопку **Выбрать**) в формате `base64-encoded X.509`. В конце процедуры необходимо нажать кнопку **Добавить**.

5.1.6 Уведомления о заблокированных письмах

Настройка позволяет задать собственный шаблон отсылаемых информационных сообщений о факте блокировки письма. Шаблон необходимо составлять в соответствии с RFC 5322.

*Примечание: если настройка выключена, то режим **Поместить в карантин и уведомить получателя** работает, как режим **Поместить в карантин**, без уведомления получателя*



Для шаблонизирования используется Jinja2-синтаксис. Ниже приведен перечень токенов, доступных для использования в поле {{ }} при составлении текста уведомления:

Переменная	Описание
from	Отправитель.
to	Получатель.
headers	Заголовки.
subject	Тема.
malicious_file_list	Список вредоносных файлов.
reason	Основная причина блокировки.
reasons	Список всех причин блокировки письма.
date	Дата получения письма системой **MXDR**.
alerts	Список всех причин вредоносности/нежелательности письма (в т.ч. не ведущих к блокировке).
is_malicious	Флаг, является ли письмо вредоносным.
is_unwanted	Флаг, является ли письмо нежелательным.
is_unwanted_phishing	Флаг, относится ли письмо к фишингу.
is_unwanted_spam	Флаг, относится ли письмо к спаму.
is_unwanted_policy	Флаг, является ли письмо нежелательным из-за нарушения политик.

Примечание: флаги можно использовать для формирования разных шаблонов для разных ситуаций с использованием синтаксиса ветвления Jinja2.

5.1.7 Настройки байпаса

В **Business Email Protection** присутствует возможность настроить таймаут анализа писем, по истечении которого письма отправляются получателю до окончания проверки.

Примечание: отправление письма до окончания анализа не означает отмену проверки. Модуль BEP продолжит проверку письма и создаст алерт, если обнаружит вредоносное содержимое.

Для настройки таймаута анализа необходимо указать требуемое значение в соответствующее поле и нажать **Сохранить**.

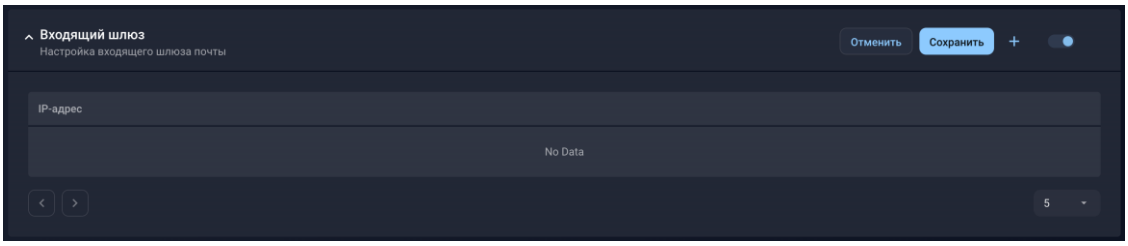
5.1.8 Входящий шлюз

В настройках **Business Email Protection** есть функция настройки входящего шлюза. Данная опция актуальна для клиентов, интегрирующих **Business Email Protection** с уже

присутствующим почтовым шлюзом. В данном блоке можно указать адреса текущей инфраструктуры для осуществления корректной проверки SPF писем. Это позволяет отказаться от обязательной смены MX-записи защищаемых доменов.

Премичание: почта с серверов клиента должна направляться на MX-записи BEP.

Для доступа к настройке необходимо переключить ползунок в правом верхнем углу блока в активное состояние.



Чтобы добавить адрес нужно нажать на plus-icon. Откроется сайдбар с областью для добавления IP-адресов.

Когда все адреса будут внесены — необходимо нажать кнопку кнопку **Добавить**. В конце, для сохранения всех изменений, в самом блоке **Входящий шлюз** нужно нажать кнопку **Сохранить**.

5.2 Политика и обнаружение

В результате анализа электронного письма может быть выявлен нежелательный контент, что приведет к активации правил, классифицирующих письмо как вредоносное или нежелательное. По завершении анализа будет выполнено действие, настроенное для соответствующего критерия блокировки. Ниже представлен список всех возможных действий:

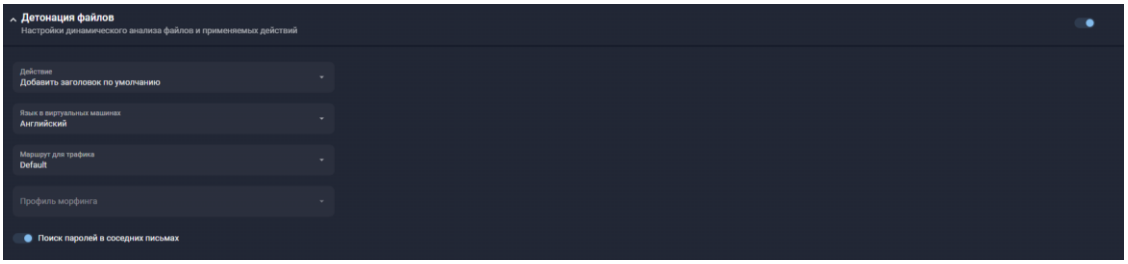
Вариант	Действие
Добавить заголовок по умолчанию	Пропустить письмо и добавить установленный по умолчанию для каждого блока настроек заголовок, который может быть отфильтрован вашим почтовым сервером.

Вариант	Действие
Добавить тег по умолчанию к теме	Пропустить письмо и добавить тег, установленный по умолчанию. Каждому блоку настроек присвоен уникальный тег.
Поместить в карантин и уведомить получателя	Блокировать письмо и уведомить об этом получателя.
Поместить в карантин	Блокировать письмо без уведомления получателя.
Сменить получателя	Пропустить письмо и отправить его другому получателю.
Добавить пользовательский заголовок	Пропустить письмо и добавить заголовок, указанный пользователем в определенной настройке.
Добавить пользовательский тег к теме	Пропустить письмо и добавить тег, указанный пользователем в определенной настройке.

 работают только при переведенном в активное состояние ползунке и являются опциональными.

5.2.1 Детонация файлов

Использование данного раздела позволяет осуществлять выбор режима для **Malware Detonation Platform**, который выполняет анализ объектов, вложенных в письма или полученных в результате исследования ссылок в письмах/вложениях.



В поле **Действие** выберите один из доступных вариантов.

- При выборе Добавить заголовок по умолчанию письмам с вредоносным содержимым будет присваиваться заголовок X-ATMOSPHERE-ANALYZE: Malicious.
- При выборе Добавить тег по умолчанию письмам будет присваиваться тег Malicious file.

По умолчанию доступен русский и английский языки виртуальных машин (при ненастроенном профиле морфинга). Для выбора иного языка необходим соответствующий настроенный профиль морфиннга. При настроенном профиле морфинга доступен расширенный список языков.

В поле **Маршрут для трафика** укажите устройство **Tunneling Exit Node** (выходной узел), через который **Business Email Protection** будет выходить в интернет для анализа ссылок и файлов в **MDP**.

Tunneling Exit Node — технология туннелирования трафика, позволяющая настраивать пользовательские выходные узлы для использования в качестве шлюзов при анализе файлов в **Malware Detonation Platform**. При использовании **Tunneling Exit Node**, облачные виртуальные машины **MDP** выпускают свой трафик через созданные в вашей инфраструктуре выходные узлы таким образом, что сетевой трафик выглядит для атакующей стороны точно также, как если бы его отправляли хосты в вашем настоящем окружении.

В поле Профиль морфинга можно задать профили, имитирующие реальную среду клиента.

5.2.1.1 Поиск паролей в соседних письмах

Дополнительно существует возможно включить функцию **Поиск паролей в соседних письмах**. При активации этой функции система будет искать пароли не только в текущем письме, но и в связанных письмах (как уже полученных, так и будущих).

5.2.2 Статический анализ файлов

Статический анализ файлов — это процесс анализа исходного кода и бинарных файлов для выявления потенциальных уязвимостей, вредоносного кода и других угроз без выполнения этих файлов.

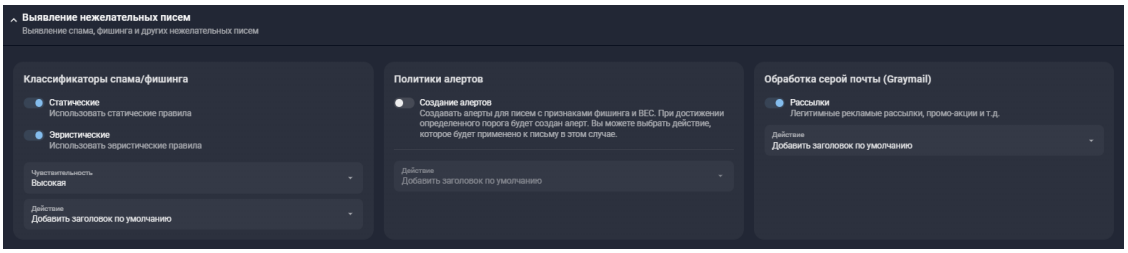
Настройка позволяет включить быстрое сканирование писем и файлов антивирусом и применять выбираемое действие в случае обнаружения угроз.

Данный блок настроек может быть включен и без включения поведенческого анализа в **Malware Detonation Platform**.

При выборе *Добавить заголовок по умолчанию* письмам с вредоносным содержимым будет присваиваться заголовок `X-ATMOSPHERE-ANALYZE: Malicious`. –

При выборе *Добавить тег по умолчанию* письмам будет присваиваться тег `Malicious file`.

5.2.3 Выявление нежелательных писем



5.2.3.1 Классификаторы спама/фишинга

Используя данную настройку, пользователь может установить фильтры на входящую почту для выявления спама, фишинга и атак типа BEC (Business Email Compromise). Письмам будут присваиваться соответствующие классификаторы и добавляться заголовки. Для выбора одного или двух классификаторов переключить нужный ползунок, чтобы привести классификатор в активное состояние.

Далее после выбора классификатора идет настройка чувствительности. В зависимости от выбранного порога чувствительности письма будут проходить соответствующую сложности проверку. Чем выше порог чувствительности - тем больше будет обнаружено нежелательных писем, которые требуют внимания.

На выбор даются следующие пороги чувствительности:

- **Низкая** - наименьший порог.
- **Средняя** - средний порог.
- **Высокая** - высокий порог.
- **Параноидальная** - наивысший порог.

В поле **Действие** можно выбрать один из доступных вариантов.

- При выборе *Добавить заголовок по умолчанию* нежелательным письмам будет присваиваться заголовок `X-Spam-Status: Yes`.
- При выборе *Добавить тег по умолчанию* письмам будет присваиваться тег `Unwanted`.

5.2.3.2 Политики алертов

В данном блоке настраивается генерация алерта. При переключении ползунка можно активировать, либо отключить функцию генерации алертов на нежелательные письма.

Алерты генерируются не на все нежелательные письма, а только на те, которые внутренний классификатор системы выделил как наиболее опасные.

В поле **Действие** можно выбрать один из доступных вариантов.

- При выборе *Добавить заголовок по умолчанию* нежелательным письмам будет присваиваться заголовок `X-Spam-Status: Yes`.
- При выборе *Добавить тег по умолчанию* письмам будет присваиваться тег `Unwanted`.

Действия в блоке *Классификаторы спама/фишинга* и блоке *Политики алертов* не суммируются. К примеру - если для классификаторов спама/фишинга выбрано действие **Добавление заголовка**, то данное действие будет присвоено только к тем письмам, для которых не был сгенерирован алерт. Если в блоке настройки Политики алертов выбрано действие **Поместить в карантин**, то данное действие будет применено ко всем письмам, для которых были сгенерированы алерты.

Рекомендованный выбор для классификаторов: Добавить заголовок по умолчанию. Это позволит сразу выявлять спам-письма и перемещать их в папку `Спам` прямо у пользователя в почтовой системе, если это было определено настройками. За пользователем сохранится возможность извлекать письма из папки `Спам`, если срабатывание было ложным и письмо переместилось туда ошибочно. Письмам, прошедшим проверку успешно, заголовок проставляться не будет.

5.2.3.3 Обработка серой почты (Graymail)

В данном блоке настраивается политика обработки рекламных писем. К серой почте относятся Легитимные рекламные рассылки, промо-акции и т.д. Для активации настройки необходимо перевести ползунок **Рассылки** в активное состояние.

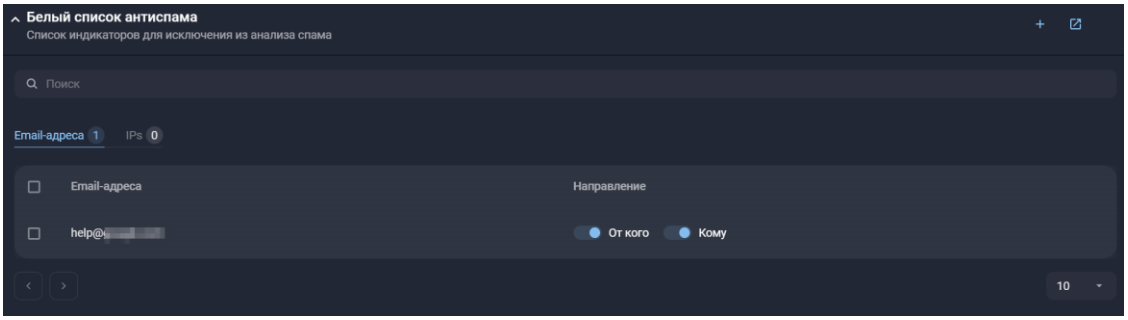
Данная настройка доступна только для нежелательных писем (тэг `Unwanted`).

В поле **Действие** можно выбрать один из доступных вариантов.

- При выборе *Добавить заголовок по умолчанию* нежелательным письмам будет присваиваться заголовок `X-Spam-Status: Yes`.
- При выборе *Добавить тег по умолчанию* письмам будет присваиваться тег `Advertisement`.

5.2.3.4 Белый список антиспама

Используя белый список антиспама, можно исключать объекты из анализа на наличие спама и фишинга в содержимом письма.



Белый список антиспама может быть создан по следующим индикаторам:

- Email-адреса
- IP-адреса (IPs)

В качестве IP используется IP-адрес сервера, с которого было принято соединение. Email-адреса берутся из параметров SMTP-сессии (MAIL FROM и RCPT TO).

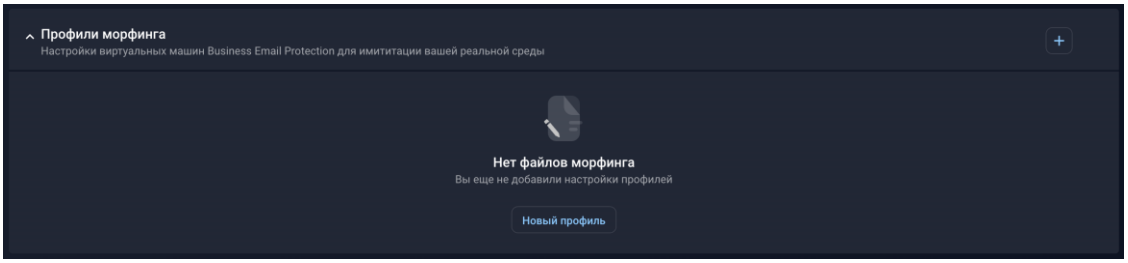
Настройки белого списка по отправителю не применятся, если письмо не прошло проверку SPF.

Данные типы записей сгруппированы по соответствующим вкладкам.

5.2.4 Профили морфинга

Профиль морфинга — это текстовый список данных позволяющий применять специфичные клиентские свойства на виртуальных машинах, используемых для анализа писем: например, присоединять виртуальные машины к контроллерам домена с конкретным именем, использовать конкретные имена пользователей и компьютеров.

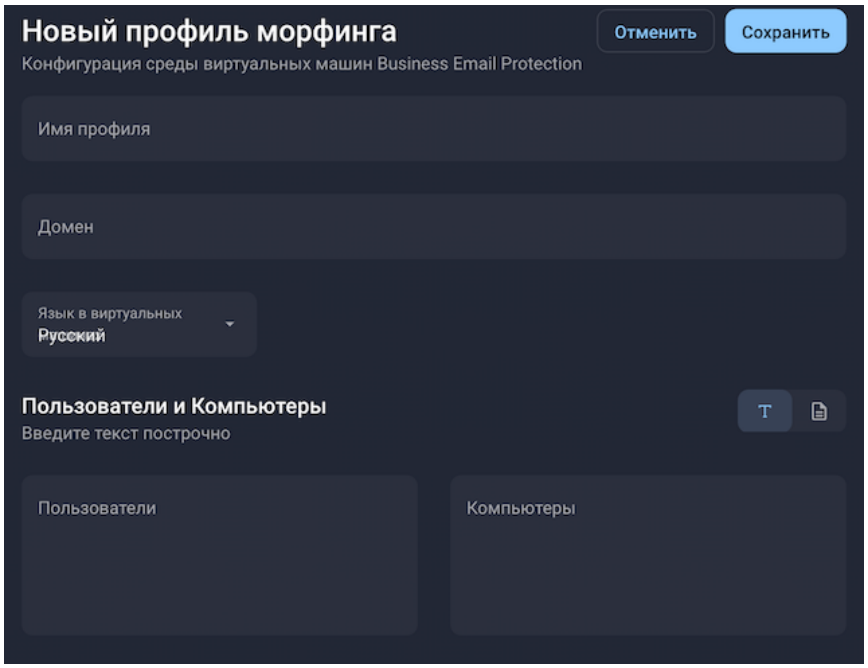
Профили морфинга позволяют имитировать доменные рабочие ПК клиента при детонации файлов в **Malware Detonation Platform**.



Для добавления новых профилей используйте соответствующие кнопки **Новый профиль** или plus-icon в правом верхнем углу настройки.

Редактировать раннее созданные профили морфинга невозможно. Чтобы внести изменения нужно создать новый профиль и по его готовности переключить все необходимые анализы на него. Старый профиль можно удалить, если необходимость в нем отпала.

Профилей морфинга может быть несколько, но активен всегда только один (выбранный).



Необходимые настройки профиля:

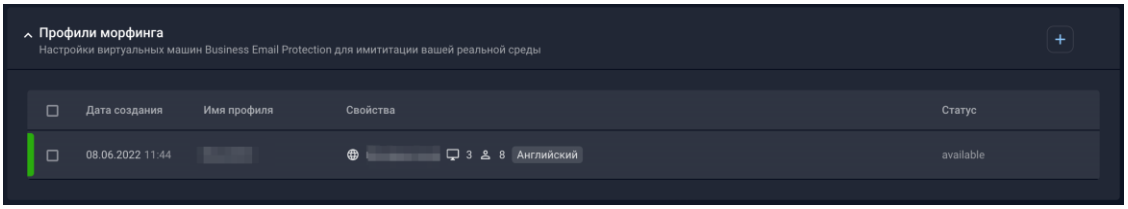
- **Имя профиля**
- **Домен** — в виде FQDN
- **Пользователи** — список имен пользователей используемых в виртуальных образах ОС MXDR Malware Detonation Platform (MDP)
- **Компьютеры** — список имён компьютеров используемых в виртуальных образах ОС MXDR Malware Detonation Platform (MDP)

Для имен пользователей и компьютеров должны учитываться **валидационные требования**. Они повторяют требования **ОС Windows**.

	Требования
Имя пользователя	- Локальные имена пользователей должны быть уникальными на автоматизированном рабочем месте - Глобальные имена - всюду по доменной области - Имя не должно быть длиннее 20 знаков - Не могут содержать знаки: **" / \ [ ] : ; | = , + * ? < >** - Имена могут содержать другие специальные знаки (пробелы, точки дефисы, подчеркивания и т.д.), но предпочтительнее этого избегать.

	Требования
Имя компьютера	- Имя компьютера не может быть длиннее 15 символов - Не может быть полностью числовым - Не может содержать следующие символы: **: ` - ! @ # $ % ^ & * ( ) = + _ [ ] { } \ | : ; , ' " . < > / ?**

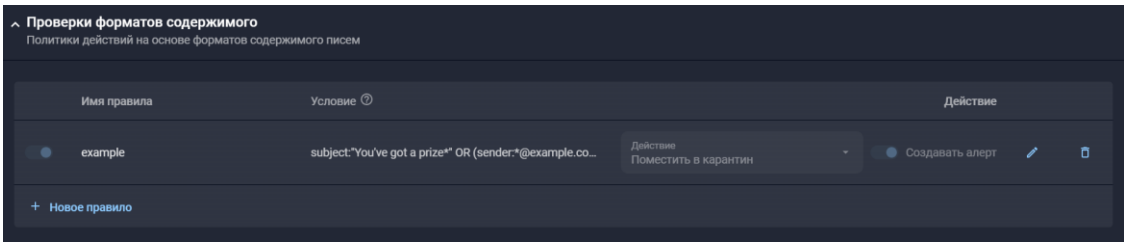
Списки имен пользователей и компьютеров выбираются случайным образом и обновляются через заданное производителем число анализов



Создание профиля морфинга является сложным процессом. Операция по созданию одного профиля может занимать до 2х часов времени.

5.2.5 Проверки форматов содержимого

Использование данного раздела позволяет осуществлять настройку политик действий на основе форматов содержимого писем.



Общая информация содержит в себе следующие параметры:

- **Имя правила** — название политики для ее дальнейшего использования.
- **Условие** — правило, на основе которого производится проверка форматов содержимого.

Доступны следующие токены:

Токен	Описание	Пример
`file_name`**Alias:**`filename`	Имена файлов (с указанием расширения).	`file_name: *.pdf OR file_name: *.exefile_name: example.docx`
`ip`*__Alias:__`ipaddressip_address`	Ip-адрес сервера, отправляющего письма.	`ip: 192.168.10.2`
`ip_net`*__Alias:__`ipnet`	Подсеть в формате `X.X.X.X/X`.	`ip_net: 192.168.2.0/22`

Токен	Описание	Пример
url**Alias:**link	Заданные ссылки.	url: https://developer.mozilla.org/*
mx***Alias:**mx_domain	MX-записи. Токен выполняет проверку принадлежности IP-адреса отправителя переданным MX адресам.	mx: mx1.hosting.reg.ru
sender**Alias:**src	Email-адрес определенного отправителя.	sender: *@example.comsender: 123@example.com
recipient**Alias:**rcpt	Email-адрес определенного получателя.	recipient: *@example.comrecipient: 123@example.com
subject	Определенная тема письма.	subject: "You've got a prize*"
header.X	Определенный заголовок письма. Под X в токене **header.X** подразумевается имя заголовка.	header.Received: "*from tcol.evil.server*"
dkim*	Результат проверки DKIM.Варианты:	dkim: false
spf*	Результат проверки SPF.Варианты:	spf: false
dmarc*	Результат проверки DMARC.Варианты:	dmarc: false
md5*	md5 хеш письма.	md5: 1a79a4d60de6718e8e5b326e338ae533
sha1*	sha-1 хеш письма.	sha1: 5fb7ba98bbf6a96d6f6d796a0f9dc09d8c626276
sha256*	sha-256 хеш письма.	sha256: 50d858e8d8d298cfac7034945221b6636e48f42f1c9b86c8a3d4dcb056a20343
hash*	Универсальный параметр включающий в себя md5, sha-1 и sha-256.	hash: 1a79a4d60de6718e8e5b326e338ae533
has_encrypted_attach*	В письме содержится зашифрованный файл.	has_encrypted_attach: truehas_encrypted_attach: false
eml_size*	Размер письма (в байтах).	eml_size: 1024eml_size > 1024
attach_size***Alias:**att_sizefile_size	Размер файла в письме (в байтах).	attach_size: 1024attach_size > 1024

Токен	Описание	Пример
attach_count***Alias:**att_countattaches_countattachesfiles	Количество файлов в письме (включая скачанные по ссылкам).	attach_count: 1attach_count > 2
link_count***Alias:**links_countlinks	Количество ссылок в письме.	link_count: 1link_count > 2
empty_body*	Тело письма пустое.	empty_body: falseempty_body: true

Токены с пометкой *** НЕ** используют синтаксис **Lucene**. Для остальных токенов можно использовать поисковые метасимволы * и ?.

? повторяет предыдущий символ ноль или один раз. Например: abc? # соответствует ab и abc.

* повторяет предыдущий символ ноль или более раз. Например: ab* # соответствует a, ab, abb, abbb и т.д.

Для токенов в одном поле **Условие** можно перечислить несколько правил. Правила прописываются в следующем формате: file_name: *имя файла*. Для перечисления нескольких правил используются операторы **AND**, **NOT** или **OR**, а также круглые скобки. Подробнее о синтаксисе и группировке нескольких правил можно узнать на официальном сайте Lucene.

Токены **eml_size**, **attach_size**, **attach_count**, **link_count** поддерживают логические операторы <, <=, ==, >, >=

Пример правила представлен ниже:

```
file_name: *.pdf OR file_name: *.exe
subject: "You've got a prize*" AND NOT sender: *@example.com
ip: 192.168.10.2 OR (ip_net:192.168.2.0/22 AND recipient:admin@example.com)
```

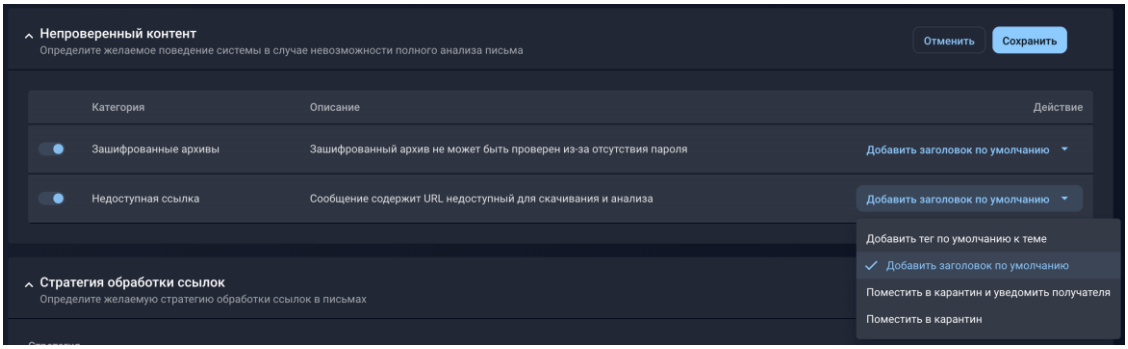
В поле **Действие** выберите один из доступных вариантов.

- При выборе *Добавить заголовок по умолчанию* нежелательным письмам будет присваиваться заголовок X-Spam-Status: Yes.
- При выборе *Добавить тег по умолчанию* письмам будет присваиваться тег Custom policy: {*имя политики*}.

Также можно создавать правила проверки форматов содержимого с помощью загрузки индикаторов компрометации из внешних систем.

5.2.6 Непроверенный контент

Использование данного раздела позволяет определять желаемое поведение системы в случае невозможности полного анализа письма.



Общая информация содержит в себе следующие параметры:

- **Категория** — категория проверяемого контента
  - **Зашифрованные архивы**
  - **Недоступная ссылка**
- **Описание** — причина, препятствующая полному анализу письма.

В поле **Действие** выберите один из доступных вариантов.

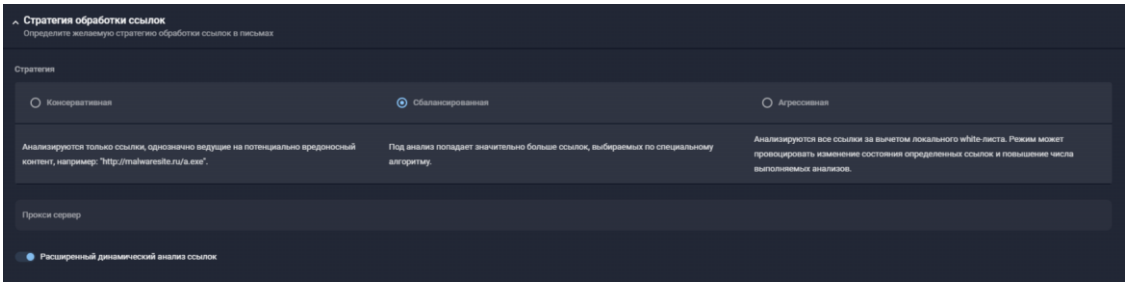
- При выборе *Добавить заголовок по умолчанию* нежелательным письмам будет присваиваться заголовок `X-Spam-Status: Yes`.
- При выборе *Добавить тег по умолчанию* письмам будут присваиваться следующие теги:
  - Для писем с зашифрованными архивам - `Encrypted archive`.
  - Для писем с недоступными ссылками - `Unavailable link`.

Если со временем удастся проверить контент, письмо может изменить статус на зелёный, а в случае блокировки, оно будет отправлено.

5.2.7 Стратегия обработки ссылок

При интеграции с почтовой системой **MXDR Business Email Protection** будет осуществлять анализ почтовых сообщений на предмет содержания в нём ссылок на внешние ресурсы. При обнаружении ссылок **Business Email Protection** будет производить переходы по ссылкам, которые система определила значимыми для анализа. Переход по ссылке ограничивается только ресурсом, указанным в ссылке. Дальнейший анализ будет зависеть от выбранной **стратегии обработки ссылок**.

Если был настроен **Tunneling Exit Node** в блоке **Детонация**, то ссылки будут скачиваться через **Tunneling Exit Node**.



Предлагаемые стратегии:

- **Консервативная** — анализируются только ссылки, однозначно ведущие на потенциально-вредоносный контент, например: http://malwaresite.ru/a.exe. Ссылки, не имеющие таких явных признаков, пропускаются.
- **Сбалансированная** — под анализ попадает значительно больше ссылок, выбираемых по специальному алгоритму. Не попадают на анализ ссылки на популярные домены и сервисы, потенциально изменяющие состояние ссылки. Этот режим работы требует настройки локального белого списка для ссылок.
- **Агрессивная** — анализируются все ссылки, за вычетом локального white-листа. Режим может провоцировать изменение состояния определенных ссылок и повышенное число выполняемых анализов.

Рекомендованный выбор стратегии обработки писем - **Сбалансированная**, т.к. переходы по ссылкам и их анализ в данном случае будет определяться высокоточным алгоритмом.

Дополнительно в поле **прокси сервер** можно указать прокси-сервер для обработки ссылок во входящих электронных сообщениях.

5.2.7.1 Расширенный динамический анализ ссылок

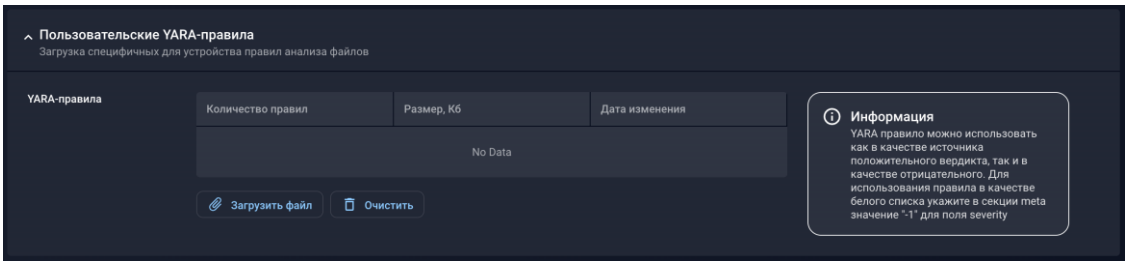
Опция отвечает за передачу в модуль **Malware Detonation Platform** результата скачивания ссылки в случае, если данный результат является HTML-страницей, а не исполняемым файлом. Это позволяет обрабатывать промежуточные страницы для загрузки файлов, однако увеличивает нагрузку и может привести к ненамеренным переходам по ссылкам на этих страницах. По умолчанию эта опция отключена.

5.2.8 Пользовательские YARA правила

Настройка позволяет добавлять в систему **YARA-правила** для дополнительных решений по обработке файлов.

Для добавления **YARA правила** необходимо загрузить его в формате текстового файла через интерфейс портала.

Можно загрузить только один файл (при загрузке нового файла старый файл будет перезаписан), но, при этом в файле может быть несколько правил одновременно.



YARA правила можно использовать как белые списки. Для использования правила в качестве белого списка укажите в секции meta значение “-1” для поля severity.

Если используется поле `severity`, то правила с `severity` ниже 4 игнорируются.

5.2.9 YARA правила

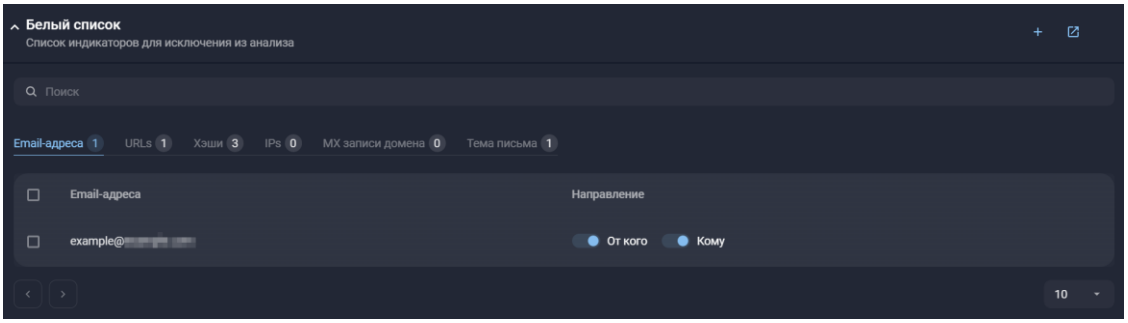
После срабатывания встроенного или пользовательского **YARA правила** с письмом будет выполнено одно из доступных действий. Для того чтобы задать это действие, нажмите кнопку переключения раздела **YARA правила** и в раскрывающемся меню **Текущая политика** выберите один из доступных вариантов.

Все случаи, в которых срабатывают одинаковые **YARA правила**, будут добавляться в один Алерт.

- При выборе *Добавить заголовок по умолчанию* нежелательным письмам будет присваиваться заголовок `X-ATMOSPHERE-ANALYZE: Malicious`.
- При выборе *Добавить тег по умолчанию* письмам будет присваиваться тег `Custom yara rule: {}`

5.2.10 Белый список

Используя белые списки, можно исключать объекты из анализа **Business Email Protection**.



Белый список можно создать по следующим индикаторам:

- **Email-адреса**
- **URLs**
- **Хэши**
- **IPs**
- **MX записи домена**
- **Тема письма**

Данные типы записей сгруппированы по соответствующим вкладкам.

В качестве IP используется IP-адрес сервера, с которого было принято соединение. Email-адреса берутся из параметров SMTP-сессии (MAIL FROM и RCPT TO). В случае выявления добавленных в белый список email-адресов или IP-адресов письма не будут проанализированы и сразу отправятся получателю. В случае файлов (хэш) - не будет проанализирован сам файл, в случае ссылок (URL) - не будет скачана сама ссылка.

Настройки белого списка по отправителю не применятся, если оно не прошло проверку SPF.

Важно понимать, что значение MAIL FROM может не совпадать со значением заголовка From. В поле “Источник” в карточке письма обычно отображается значение MAIL FROM, однако если отправитель оставил его пустым (<>), в поле “Источник” будет отображено значение из заголовка From, а белый список по отправителю применить будет невозможно.

5.2.10.1 Работа с белыми списками

Для работы с блоками настроек **Белый список антиспама** и **Белый список** следуйте шагам, описанным ниже:

1. Перейдите в **Настройки** → **Модули**, выберите **Business Email Protection** и нажмите **Основные настройки**.

2. Перейдите во вкладку **Политика и обнаружение** и выберите интересующую вас настройку: **Белый список антиспама** или **Белый список**. Если список пуст, появится сообщение *Список пуст*. Иначе, появится существующий список объектов.

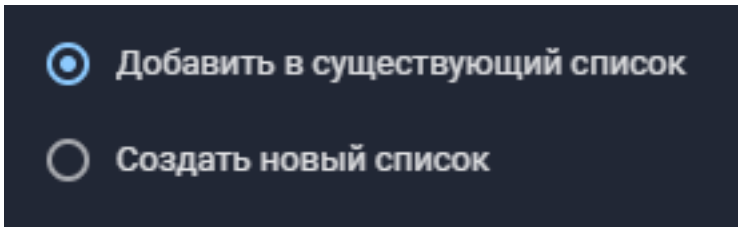
3. Нажмите *Добавить* или +, затем выберите тип записи, которую необходимо добавить в белый список. Для Белого списка антиспама это поля Email-адреса и IPs. Для Белого списка - Email-адреса, URLs, Хэш-функции, IP-адреса, MX записи домена и Тема письма.

4. Заполните обязательные поля:

Тип записи	Поля
Email-адреса	Поле для записи Email-адресов построчно.
URLs	Ссылки на веб-ресурсы построчно.
Хэш-функции	Для каждого типа хешей - MD5, SHA1, SHA256 - отдельное поле для записи построчно.
IPs	Поле для записи IP-адресов построчно.
MX записи домена	Поле для внесения MX записей построчно.
Тема письма	Поле для введения интересующих тем письма построчно.

Вы можете добавлять записи, указывая их построчно или загружать их в файле с расширением **.txt**. Для составления списка можно использовать регулярные выражения. Чтобы загрузить файл нажмите file-icon и перетащите необходимый файл или выберите его в проводнике.

5. Решите, хотите ли Вы добавить записи в существующий список или создать новый, и нажмите соответствующую кнопку.



Если Вы добавляете IPs URLs, Хэш-функции, MX записи домена или Темы письма то перейдите к шагу 7.

6. Если Вы добавляете Email-адреса, выберите направление анализа для электронных писем:

- **От кого** — искать в отправителе.
- **Кому** — искать в получателе.

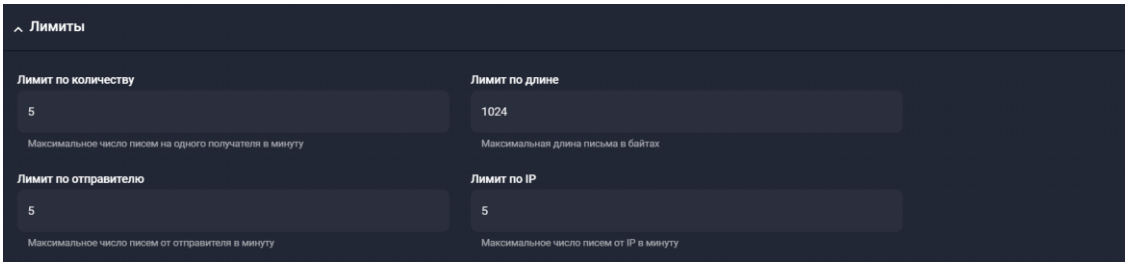
Вы можете выбрать одну и обе опции.

7. Нажмите *Добавить* в правом верхнем углу.

Соответствующие записи появятся в списке.

5.2.11 Лимиты

Раздел позволяет настроить дополнительные лимиты на получение электронной почты.



Лимиты позволяют предотвратить спам и поддерживать производительность и безопасность почтовых систем.

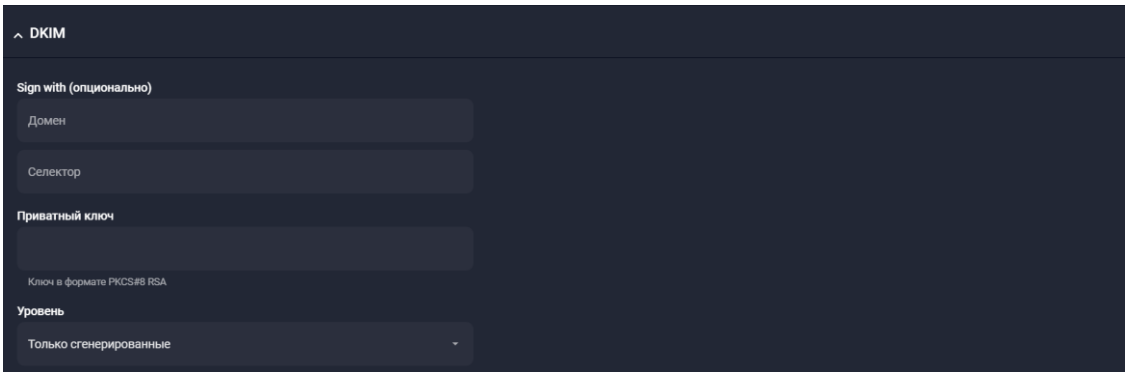
Необходимые настройки:

- **Лимит по количеству** — определяет, сколько писем можно отправить одному получателю за одну минуту. *По умолчанию: 100 писем в минуту*.
- **Лимит по отправителю** — ограничивает количество писем, которые один отправитель может отправить за одну минуту. *По умолчанию: 100 писем в минуту*.
- **Лимит по длине** — устанавливает максимальный размер письма, включая все вложения и форматирование (в байтах). *По умолчанию: 52 428 800 байт*.
- **Лимит по IP** — ограничивает количество писем, которые могут быть отправлены с одного IP-адреса за одну минуту. *По умолчанию: 100 писем в минуту*.

Для on-prem версии поля по умолчанию имеют значение **None**.

5.2.12 DKIM

Раздел DKIM (DomainKeys Identified Mail) предназначен для настройки подписи отправленных писем.



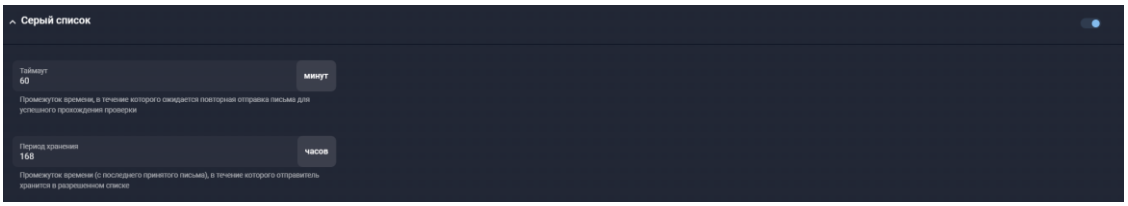
По умолчанию в полях используются ключи для подписи DKIM от компании АО «БУДУЩЕЕ». По необходимости подпись может осуществляться с использованием кастомных ключей. Для этого необходимо самостоятельно заполнить соответствующие поля.

Необходимые настройки:

- **Домен (опционально)** — домен, для которого будет использоваться DKIM. Это поле не является обязательным.
- **Селектор (опционально)** — селектор DKIM. Селектор помогает идентифицировать набор ключей DKIM, используемых для конкретного домена.
- **Приватный ключ** — приватный ключ в формате PKCS#8 RSA. Этот ключ используется для подписи сообщений и должен быть защищён.
- **Уровень** — уровень использования DKIM. Возможные значения:
  - **Подписывать все письма** — подписывать все исходящие письма.
  - **Только модифицированные и сгенерированные** — подписывать только те письма, которые были изменены или сгенерированы системой.
  - **Только сгенерированные** — подписывать только те письма, которые были сгенерированы системой.
  - **Не подписывать письма** — не использовать DKIM для подписания писем.

5.2.13 Серый список

Серый список (Greylisting) — это метод защиты электронной почты от спама, который временно отклоняет все электронные письма от неизвестных отправителей. Основная идея заключается в том, что легитимные почтовые серверы повторно отправляют сообщения после короткой задержки, в то время как многие спам-серверы этого не делают. Для активации функции переведите ползунок в активное состояние.



Необходимые настройки:

- **Таймаут** — промежуток времени (в минутах), в течение которого ожидается повторная отправка письма для успешного прохождения проверки. *Значение по умолчанию: 60 минут.*
- **Период хранения** — промежуток времени (в часах), в течение которого отправитель хранится в разрешенном списке с момента последнего принятого письма. *Значение по умолчанию: 168 часов*

Таймаут — если отправитель не повторит попытку отправки письма в течение указанного таймаута, письмо будет отклонено.

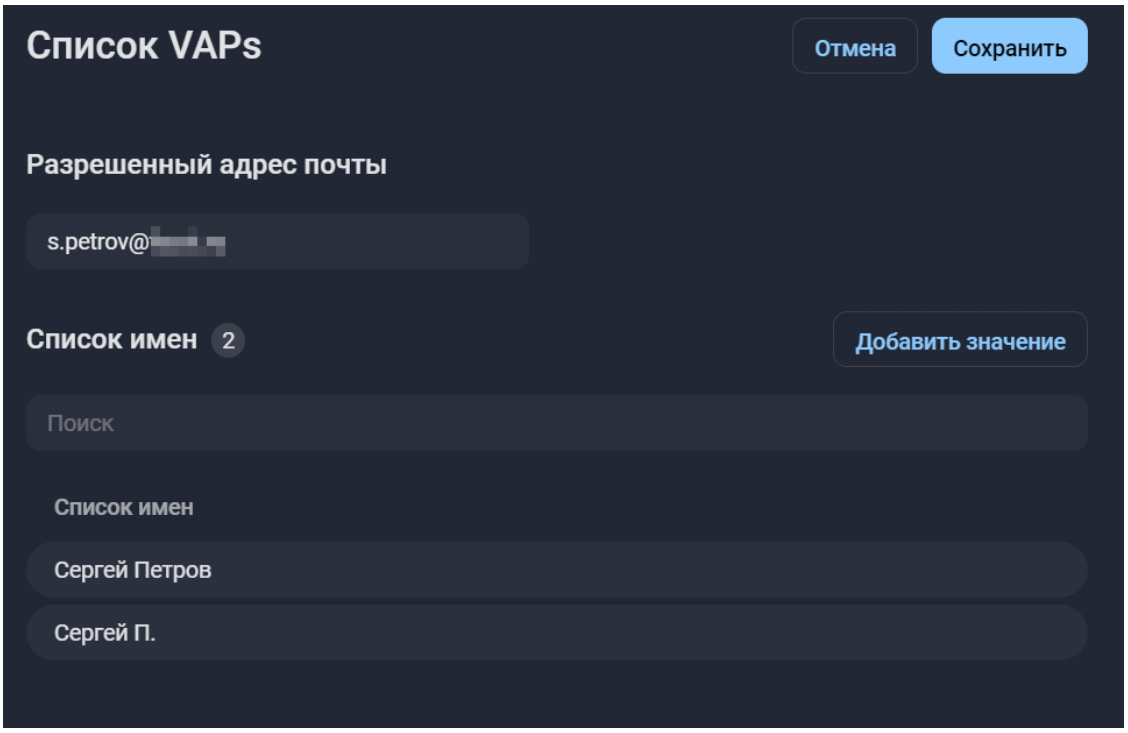
Период хранения — по истечении этого времени отправитель должен будет снова пройти проверку серого списка при отправке нового письма.

5.2.13.1 Список VAPs

Управление списком **VAPs (Very Attacked Persons)** — в список вносятся данные сотрудников, за которых с наибольшей вероятностью могут выдавать себя злоумышленники.

5.2.13.2 Настройка карточки сотрудника

Настройка списка предполагает настройку карточки соотношения email сотрудника и его подписи:



В каждой карточке сотрудника нужно перечислить два списка сущностей: отображаемых имен и почтовый адрес. Это позволит системе антиспама проверять соответствие отображаемого имени и email-адреса для предотвращения фишинговых атак.

Если сотруднику отправят письмо с отображаемым именем “Иван Иванов”, но письмо придет не с адреса i.ivanov@example.ru, система антиспама отметит это письмо как подозрительное.

6 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка осуществляется в соответствии с условиями контракта следующими способами:

- Приоритетный способ осуществления техподдержки через создание запросов во вкладке «Поддержка» по ссылке https://xdr.f6.security/service-desk
- по электронной почте: info@f6.ru;
- по номеру телефона: +7 495 984-33-64;

В рамках технической поддержки оказываются следующие услуги:

- консультация по фактическому наличию имеющегося функционала в системе;
- помощь в настройке и интеграции ПО;
- помощь в эксплуатации ПО;
- решение технических проблем;
- пояснение принципов работы имеющихся механизмов ПО;
- поиск, тестирование и фиксирование найденных ошибок;
- предоставление актуальной документации по настройке, эксплуатации и работе ПО.

Время работы технической поддержки: с понедельника по пятницу с 9:00 до 18:00 UTC+3.

Фактический адрес размещения службы поддержки ПО «F6 Business Email Protection»: 115088, г. Москва, ул. Шарикоподшипниковская, д. 1.