

Positive Technologies

Anti-APT

Версия 1.0



Руководство оператора

POSITIVE TECHNOLOGIES

© АО "Позитив Текнолоджиз", 2019.

Настоящий документ является собственностью АО "Позитив Текнолоджиз" (далее – "Позитив Текнолоджиз") и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения "Позитив Текнолоджиз".

Документ может быть изменен без предварительного уведомления.

Positive Technologies, Positive Hack Days, PTSECURITY, MaxPatrol, XSpider, SurfPatrol, N-Scope, Positive Technologies Application Firewall, Positive Technologies Application Inspector, Positive Technologies MultiScanner, Positive Technologies Reporting Portal являются зарегистрированными товарными знаками либо товарными знаками "Позитив Текнолоджиз".

Иные товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям. "Позитив Текнолоджиз" не аффилировано с такими правообладателями и не производит продукцию, маркированную такими знаками.

Дата редакции документа: 26.07.2019

Содержание

1.	Об этом документе	4
2.	О РТ Anti-APT.....	5
3.	Вход в РТ Anti-APT.....	6
4.	Работа с РТ MS.....	8
5.	Работа с РТ NAD	9

1. Об этом документе

Руководство оператора безопасности содержит ссылочную информацию об использовании Positive Technologies Anti-APT (далее также – PT Anti-APT) для управления событиями информационными безопасности. Руководство не содержит инструкций по установке, первоначальной настройке и администрированию PT Anti-APT.

Руководство адресовано руководителям и специалистам, ответственным за обеспечение информационной безопасности, контроль и расследование инцидентов.

Комплект документации PT Anti-APT включает в себя следующие документы:

- Этот документ.
- Руководство по установке PT Anti-APT – содержит информацию, касающуюся установки PT Anti-APT.
- Руководство администратора PT MS – содержит справочную информацию и инструкции по установке, настройке и администрированию PT MS.
- Руководство администратора PT NAD – содержит справочную информацию и инструкции по установке, настройке и администрированию PT NAD.
- Руководство оператора безопасности PT MS – содержит сценарии использования PT MS для управления событиями информационной безопасности.
- Руководство оператора безопасности PT NAD – содержит сценарии использования PT NAD для управления информационными активами организации и событиями информационной безопасности.

2. О PT Anti-APT

Positive Technologies Anti-APT (далее также – комплекс, PT Anti-APT) – программный комплекс, предназначенный для раннего выявления сложных угроз и сокращения присутствия злоумышленника в инфраструктуре. Комплекс позволяет максимально быстро обнаружить присутствие злоумышленника в сети и воссоздать полную картину атаки для детального расследования. Цели применения комплекса:

- предотвратить проникновение в инфраструктуру через основные векторы атак;
- максимально быстро выявлять присутствие злоумышленника в сети;
- повысить эффективность расследований благодаря возможности детально восстановить путь перемещения злоумышленника в сети;
- выявлять слабые места защиты и получать экспертные рекомендации для повышения уровня защищенности.

3. Вход в PT Anti-APT

Сервис управления пользователями и доступом Positive Technologies Identity and Access Management (PT IAM) обеспечивает механизм единого входа (технология single sign-on) в приложения "Позитив Текнолоджиз".

Перед входом в PT Anti-APT запросите у администратора PT Anti-APT:

- ссылку для входа в интерфейс PT IAM;
- логин и пароль вашей учетной записи пользователя.

Перед выполнением инструкции вам нужно убедиться, что в браузере разрешены всплывающие окна.

► Чтобы войти в PT IAM:

1. В адресной строке браузера введите ссылку для входа в интерфейс PT IAM.
Откроется страница входа в сервис PT IAM.

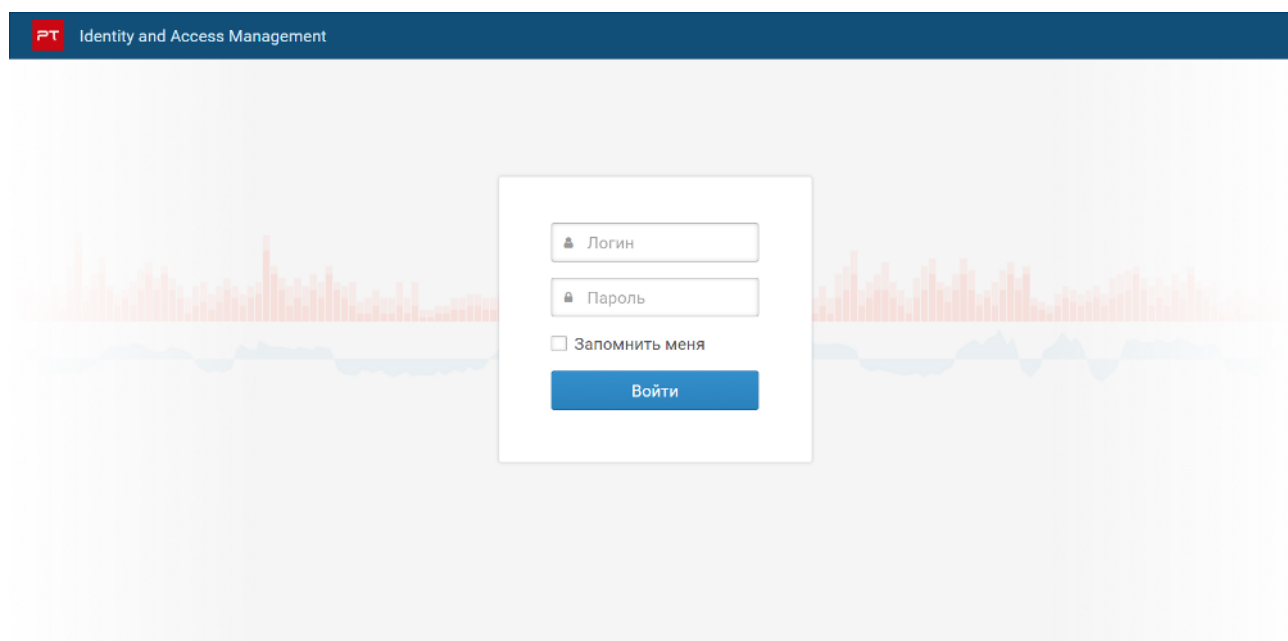


Рисунок 1. Ввод учетных данных

2. В поле **Пароль** введите пароль вашей учетной записи.
3. Нажмите кнопку **Войти**.

Система проверит введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница PT IAM. Если вы указали неверные данные, отобразится сообщение об ошибке.

▶ Чтобы перейти в интерфейс нужного продукта:

1. Нажмите кнопку  главного меню РТ IAM.

Откроется главное меню РТ IAM.

2. Выберите пункт с названием продукта.

Переход в интерфейс продукта выполнен.

4. Работа с PT MS

Пошаговые инструкции и информацию об использовании PT MS смотрите в Руководстве оператора PT MS.

5. Работа с PT NAD

Пошаговые инструкции и информацию об использовании PT NAD смотрите в Руководстве оператора PT NAD.

О компании

"Позитив Текнолоджиз" — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения "Позитив Текнолоджиз" для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты "Позитив Текнолоджиз" заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.