StationGuard

Кибербезопасность и функциональный мониторинг энергосистем

Информационная безопасность подстанций

За последние годы значительно возросло количество кибератак на ключевые системы управления промышленных предприятий и энергоснабжающих компаний. Поэтому многие энергопредприятия начали внедрять процессы, которые позволяют снизить риск кибератак. До недавнего времени эти процессы внедрялись главным образом в информационных сетях и центрах управления. Однако злоумышленники также могут атаковать и сети подстанций. Вследствие этого процессы эксплуатации и обслуживания этих подстанций также должны быть включены в оценку рисков для кибербезопасности.

Чтобы полностью защитить подстанции от кибератак, стратегия безопасности должна охватывать все уровни. Концепция безопасности подстанций предусматривает контроль физического и мониторинг цифрового доступа, а также мониторинг подозрительной или запрещенной активности в сети. Для этого требуются системы, обеспечивающие высокий уровнь защиты при минимальных требованиях к техническому обслуживанию и с длительным сроком службы. Кроме того, они должны легко интегрироваться с рабочими процессами эксплуатации и технического обслуживания.

Брандмауэр

Брандмауэры обеспечивают, что лишь специальные оконечные устройства могут взаимодействовать с устройствами на подстанции и только по разрешенным протоколам. Однако существуют способы их обойти.

Точки атаки в обход межсетевых экранов:

Удаленный доступ для технического обслуживания и управления.

Компьютеры для технического обслуживания, подключенные к сети или напрямую к IED.

Компьютеры для тестирования, подключенные к подстанционной шине.

Файлы, которые передаются на ПК, используемые на подстанции.

Незащищенная зона

- Критически важные системы, которые должны стабильно обмениваться данными
- Необновленные IED: обновления зачастую нельзя быстро установить, так как это затратная и трудоемкая задача
- Устаревшие устройства с уязвимостями системы безопасности, но без доступных обновлений

Брандмауэры не обеспечивают абсолютную защиту

Существует множество способов обхода брандмауэров. На многих подстанциях считывание данных регистраторов аварийных событий или обслуживание терминалов выполняются через удаленный доступ. Эти подключения создают путь, по которому вредоносное ПО может проникнуть в устройства на подстанции.

Компьютеры, используемые для технического обслуживания или тестирования, также являются целью атак. Такие ПК подключаются ко всей сети либо напрямую к отдельным устройствам защиты или управления.

Глубокоэшелонированная защита

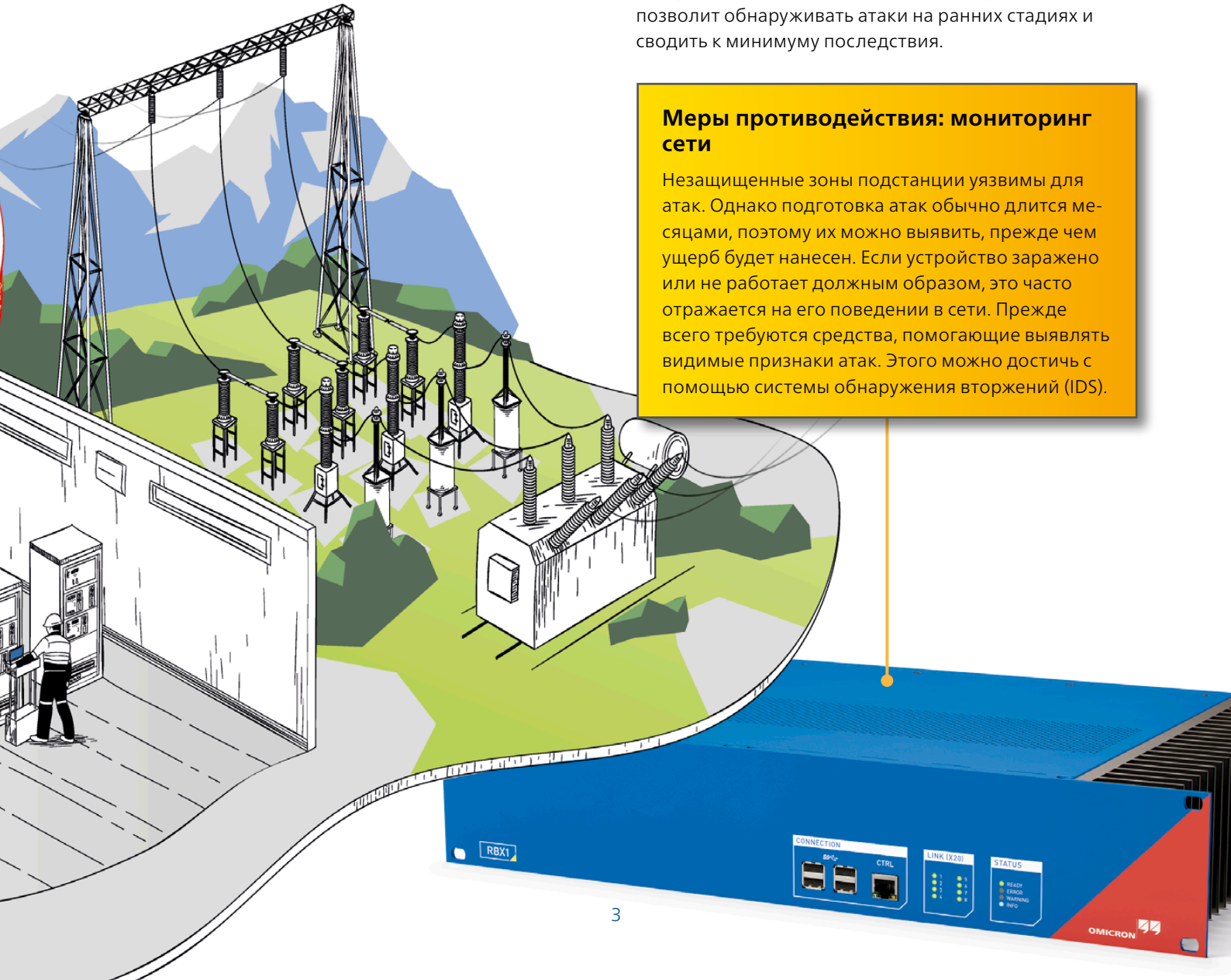
Принцип глубокоэшелонированной защиты, изложенный в стандарте IEC 62443, рекомендует не только принять меры по «укреплению оболочки», но и обеспечить несколько защитных слоев и уровней резервирования для зонированного обеспечения безопасности.

Одной из мер защиты является своевременная установка обновлений безопасности для IED. Однако эта процедура является трудоемкой и затратной, поэтому обновления не всегда удается установить быстро. Модернизировать устаревшие устройства зачастую невозможно, поскольку производитель больше не предоставляет обновления.

Поэтому важно постоянно наблюдать за устройствами, которые нельзя защитить должным образом. Это позволит обнаруживать атаки на ранних стадиях и сводить к минимуму последствия.

Меры противодействия: мониторинг сети

Незащищенные зоны подстанции уязвимы для атак. Однако подготовка атак обычно длится месяцами, поэтому их можно выявить, прежде чем ущерб будет нанесен. Если устройство заражено или не работает должным образом, это часто отражается на его поведении в сети. Прежде всего требуются средства, помогающие выявлять видимые признаки атак. Этого можно достичь с помощью системы обнаружения вторжений (IDS).



Как работает система обнаружения вторжений (IDS)

Работа систем обнаружения вторжений, как правило, основывается на одном из двух подходов:

1. Подход, основанный на сигнатурах («черный список»)

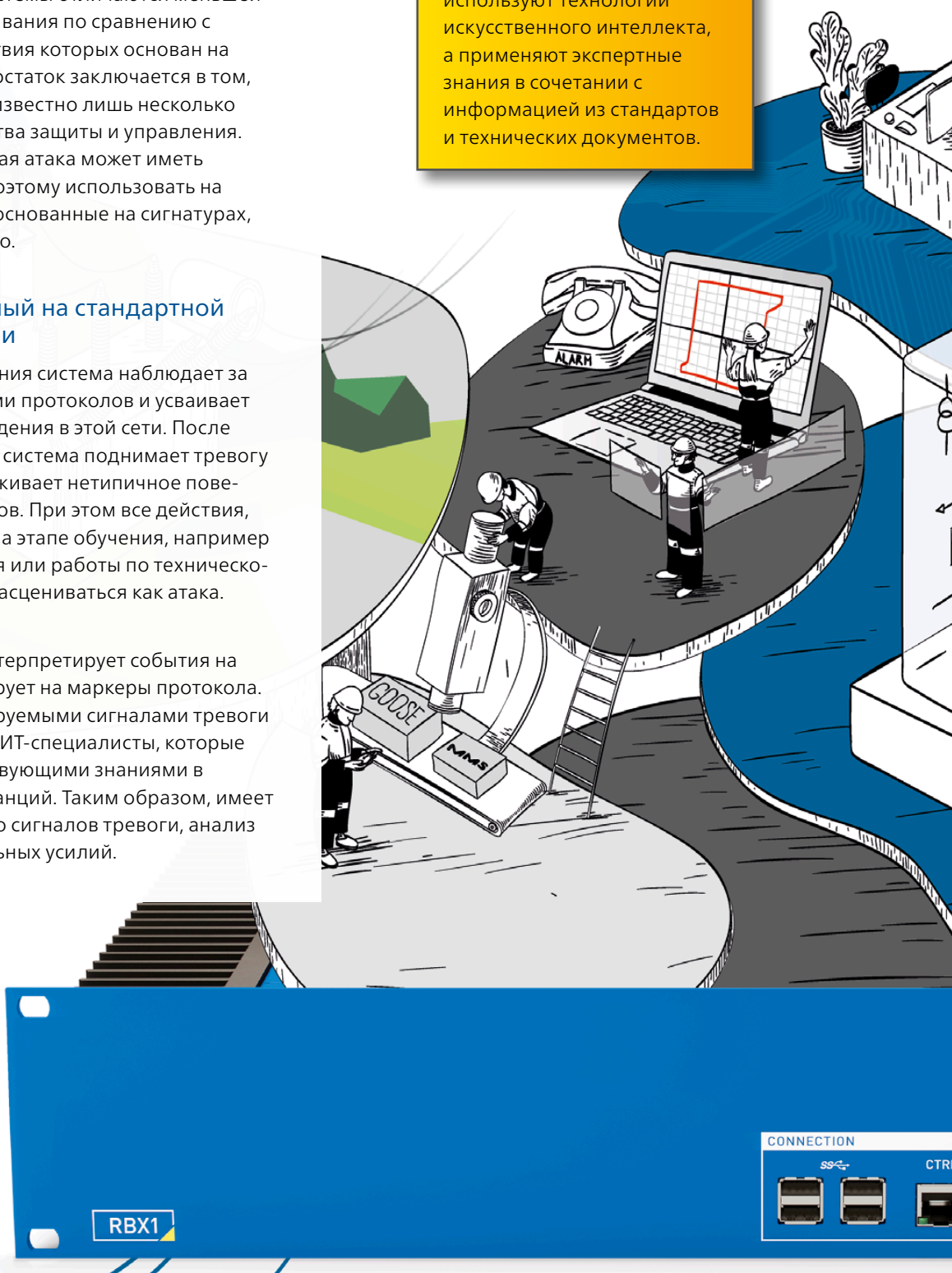
IDS сканирует сеть на наличие шаблонов известных атак. Такой подход также используется антивирусными сканерами. Такие системы отличаются меньшей частотой ложного срабатывания по сравнению с системами, принцип действия которых основан на обучении. Главный их недостаток заключается в том, что на сегодняшний день известно лишь несколько примеров атак на устройства защиты и управления. При этом даже самая первая атака может иметь серьезные последствия, поэтому использовать на подстанциях технологии, основанные на сигнатурах, практически неоправданно.

2. Подход, основанный на стандартной модели / обучении

В течение фазы обучения система наблюдает за определенными маркерами протоколов и усваивает стандартную модель поведения в этой сети. После начальной фазы обучения система поднимает тревогу каждый раз, когда обнаруживает нетипичное поведение маркеров протоколов. При этом все действия, которые не выполнялись на этапе обучения, например коммутация оборудования или работы по техническому обслуживанию, будут расцениваться как атака.

Кроме того, система не интерпретирует события на подстанции, а лишь реагирует на маркеры протокола. Это означает, что с формируемыми сигналами тревоги могут разобраться только ИТ-специалисты, которые также обладают соответствующими знаниями в области устройства подстанций. Таким образом, имеет место большое количество сигналов тревоги, анализ которых требует значительных усилий.

В системе StationGuard не используют технологии искусственного интеллекта, а применяют экспертные знания в сочетании с информацией из стандартов и технических документов.



3. Подход StationGuard

Подстанции и SCADA являются детерминистическими системами, что означает, что поведение подстанций и систем SCADA четко определено во всех случаях, даже при аварийных событиях, например, при работе устройств релейной защиты.
Основываясь на данной характеристике, к обнаружению кибератак можно применить совершенно новый подход: Имея данные о функции каждого устройства, StationGuard создает комплексную модель всей системы автоматизации, а затем сравнивает каждый сетевой пакет с этой действующей моделью. Это соответствует подходу, в котором используется список разрешенных действий («белый список»), описывающий все допустимое поведение, а на любое отклонение от него система по умолчанию выдает сигнал тревоги. Используя такой подход, можно выявлять и атаки совершенно новых типов.

Список разрешенных действий StationGuard очень подробный. Даже величины сигналов в сообщениях оценивают с помощью этой комплексной модели. Это позволяет выявлять не только киберугрозы и запрещенную активность, но и проблемы в системе автоматизации и функциях SCADA. Вот почему такая комбинация обнаружения вторжений и функционального мониторинга получила название «Мониторинг функциональной безопасности». Мы работаем над этой технологией с 2010 года. Система StationGuard столь эффективна именно благодаря интеграции знаний из области энергосистем и методов обеспечения безопасности.

Настройка системы StationGuard не предусматривает этапа обучения и требует лишь ввода пользователем небольшого объема информации с описанием назначения каждого устройства. На подстанциях IEC 61850 этот процесс можно существенно ускорить путем импорта файлов SCL.

Преимущества

- Малое количество ложных оповещений, так как StationGuard хорошо «информирована» о процессах, происходящих в энергосистемах
- Понятные сигналы тревоги, интерпретация которых не требует знания протокола
- Надежное обнаружение несанкционированных действий

Подход StationGuard, основанный на разрешенном (белом) списке

Скрупулезная проверка безопасности

Мониторинг и подробная проверка всего сетевого трафика позволяет StationGuard обнаруживать не только угрозы в системе IT-безопасности, такие как незаконные коды и несанкционированные операции управления, но и ошибки обмена данными, проблемы синхронизации и другие неисправности на подстанции. Если еще и загрузить однолинейную схему подстанции, то ограничений по глубине мониторинга практически не будет.

Пример: Сейчас StationGuard распознает 35 кодов ошибок для GOOSE-сообщений: от ошибок в порядковых номерах до слишком длинных задержек при передаче сообщений. Во втором случае регистрируется время поступления пакетов и сравнивается с временными отметками событий в сообщениях. Если полученное значение превышает предусмотренное стандартом IEC 61850-5, StationGuard отправляет сообщение о возможных проблемах обмена данными с устройством IED или сетью либо об ошибке синхронизации.

Кроме того, StationGuard сообщает о критических состояниях и потенциально опасных ошибках кодирования по множеству других протоколов OT.

Такой подробный анализ осуществляется и по другим протоколам ИТ/ОТ..

Коммуникация по протоколам MMS, IEC 60870-5-104 и DNP3

StationGuard «знает», какими функциями управляют конкретные точки данных (data points). Например, одна и та же команда может использоваться для управления силовым выключателем, переключателем ответвлений и для изменения режима тестирования устройства. Результат для подстанции в каждом случае будет совершенно разным. Система StationGuard способна разграничивать такие нюансы и «знает», какое устройство чем может управлять и в какой ситуации. Эти подробные разрешения задокументированы, их можно просмотреть в StationGuard.

Прочие протоколы

StationGuard выполняет глубокую проверку пакетов во множестве протоколов энергосистем и классических ИТ-протоколов. Используя эту функцию, система StationGuard обнаруживает не только нарушения кодирования в этих протоколах, но и такие ситуации, когда номера портов, например удаленных подключений, захвачены непредусмотренными приложениями (подмена портов).

Поддерживаемые протоколы (глубокий анализ пакетов, DPI)

- IEC 61850
- IEC 60870-5-104
- DNP3
- PRP/HSR
- Modbus TCP
- Synchrophasor
- DLMS/COSEM
- AMI
- TASE.2/ICCP
- FTP
- HTTP
- RDP
- NTP
- ARP, DHCP, ICMP
- MySQL, MS SQL, PostgreSQL
- HTTPS, SSH (выявление приложений, без расшифровки)
- telnet
- RIPv2
- SSDP
- ...

Преимущества

> Каждый пакет сравнивается с моделью системы (списком разрешенных действий).

> Выявляются не только угрозы кибератак, но и проблемы функционирования и коммуникации.

> StationGuard контролирует безопасность функционирования всех коммуникаций на подстанции и в системе SCADA.

Специализированное решение для энергосистем

Для настройки, эксплуатации и обслуживания стандартных систем обнаружения вторжений (IDS) требуются ИТ-специалисты, а также специалисты в сфере автоматизации и управления. Чтобы вовремя реагировать на аварийные сообщения, эти специалисты должны работать круглосуточно. Связанные с этим расходы будут неподъемными для большинства энергопредприятий. StationGuard представляет собой новый альтернативный вариант защиты, требующий лишь минимального обслуживания.

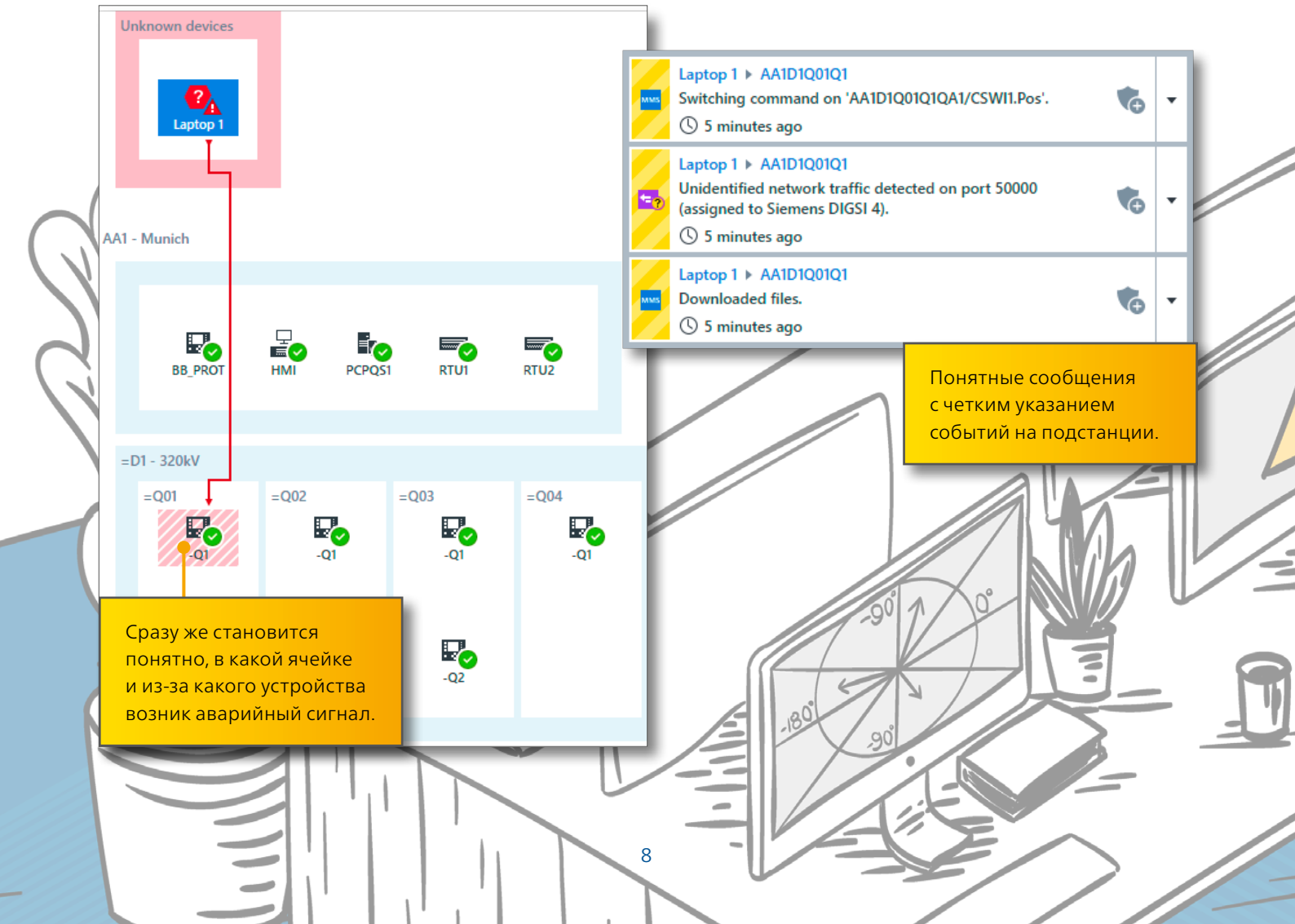
StationGuard «знает» о типовых функциях подстанций и о предусмотренном использовании ИТ-оборудования, например компьютеров для техобслуживания и тестирования. Поскольку вся эта информация доступна в автоматическом режиме, настройка StationGuard для эксплуатации в стандартном режиме не занимает много времени.

Установка

После подключения StationGuard к портам зеркалирования на сетевых коммутаторах система обнаруживает все устройства, обменивающиеся данными в этой сети.

Для подстанций IEC 61850 можно импортировать инжиниринговые файлы SCL, которые позволяют автоматически идентифицировать все IED и интегрировать их в схему подстанции. Если обмен данными не соответствует файлу SCL, StationGuard сообщает об ошибках конфигурации IEC 61850. Это особенно важно на этапе приемочных испытаний на заводе и объекте.

Для подстанций или систем SCADA, использующих протоколы IEC 60870-5-104, DNP3 либо Modbus, устройства IED и RTU можно классифицировать вручную по предварительно заданным правилам с помощью нескольких щелчков мышью. После этого любому оставшемуся ИТ-оборудованию можно присвоить соответствующую роль, например коммутатора или ПК техобслуживания. Эти роли также можно адаптировать.



Обычный режим работы

Анализируя все коммуникации, StationGuard располагает точными данными о том, какая информация может или не может передаваться в данный момент, каким устройствам сейчас разрешено быть активными, какие команды управления разрешены и надо ли реагировать на них, какие измеренные значения передаются, корректно ли время передачи сообщений. Это позволяет обнаруживать любые вероятные проблемы с IED или сетью на ранней стадии, даже до выхода компонентов из строя.

Комплексный подход к мониторингу функционирования и безопасности не имеет аналогов и предоставляет гораздо больше преимуществ, чем обычно ожидается от системы обнаружения вторжений (IDS).

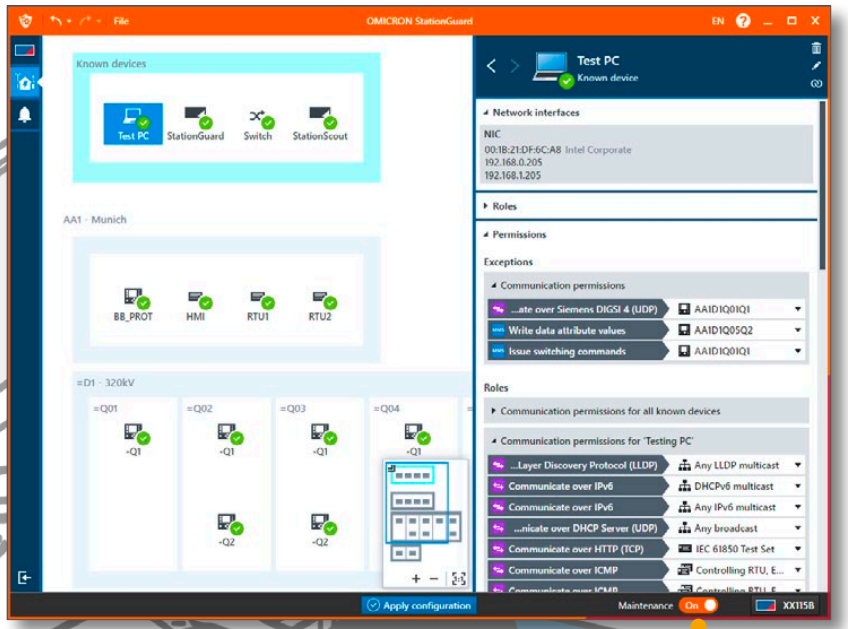
Графический интерфейс StationGuard соответствует стандартным схемам в документации и представлению событий на дисплее контроллеров подстанции, поэтому инженеры РЗиА смогут быстро понять, в чем проблема, и решить ее.

Работа в режиме «Наладка и обслуживание»

Испытания и техническое обслуживание оборудования не должны прерываться ошибочными сигналами тревоги, но и снижать уровень защиты на это время тоже рискованно. Чтобы удовлетворить эти требования, в системе StationGuard предусмотрен режим обслуживания (maintenance mode). Работы по техническому обслуживанию и испытания будут разрешены только когда этот режим активирован.

Во многих сценариях атак используются уязвимости в протоколе производителя оборудования или веб-интерфейсах. Поэтому StationGuard разрешает обмен данными с инструментами производителя только в режиме обслуживания и поднимает тревогу, если это происходит во время обычной работы. ПК техобслуживания и испытательные комплекты можно зарегистрировать в StationGuard до начала их использования, чтобы плановые задачи выполнялись без ложных срабатываний.

Уровень безопасности во время испытаний не снижается: Если зараженный испытательный ПК выполняет подозрительные действия по обмену данными, система тут же сообщает об этом.



Определенные действия разрешены только в режиме техобслуживания.

Преимущества

- Простота настройки
- Отсутствие ложных сигналов тревоги во время обычных испытаний при высоком уровне безопасности
- Отсутствие этапа обучение, обеспечение мгновенной защиты

Ускоренная реакция благодаря понятным предупреждающим

Надежная идентификация причин сигналов тревоги

Сигналы, выдаваемые системой безопасности, должны помогать оператору, а не вносить дополнительную путаницу. Именно поэтому StationGuard отображает сигналы тревоги не только в списке событий, но и на общей схеме в графическом виде. События энергосистемы, связанные с сетевыми пакетами, идентифицируются и отображаются с помощью понятной терминологии.

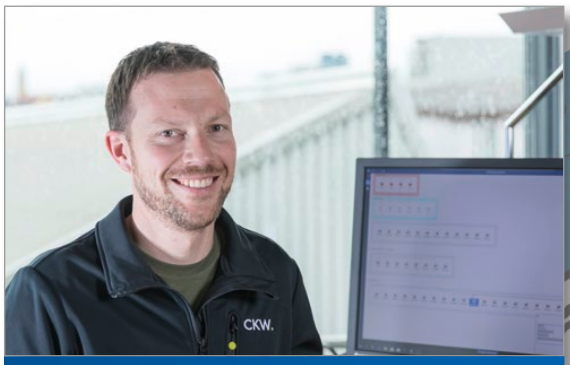
Рассмотрим следующий пример: Испытательный ПК осуществляет попытку управления силовым выключателем с помощью протокола MMS. Уведомление об этом инциденте будет содержать не протокольные термины, а четкое описание происшествия на подстанции. Из уведомления оператор сможет узнать о самом событии и о том, каким устройством вызвано.

Благодаря этому специалисты отдела ИТ-безопасности, а также инженеры по SCADA и РЗА могут общими усилиями эффективно определять причины поступления сигналов тревоги. Эта система IDS так же понятна инженерам, как журнал эксплуатации, список событий или список предупреждений на дисплее контроллера станции.

Анализ и пересылка сигналов тревоги

Простой способ интегрировать систему StationGuard в подстанции старого образца — использовать двоичные выходы платформы RBX1. Присутствие неквитированного аварийного сигнала сигнализируется двоичными выходами, которые могут быть подключены к RTU и интегрированы в список сигналов SCADA.

Как вариант, наши понятные предупреждающие сообщения можно пересылать с помощью протокола Syslog. Доступны различные встраиваемые модули для интеграции StationGuard в системы безопасности и управления событиями (SIEM), а также в системы обработки заявок различных разработчиков.



«Работать со StationGuard действительно просто. Информация излагается понятно и без ИТ-жаргона. И все это в сочетании с высоким качеством OMICRON, к которому мы привыкли.»

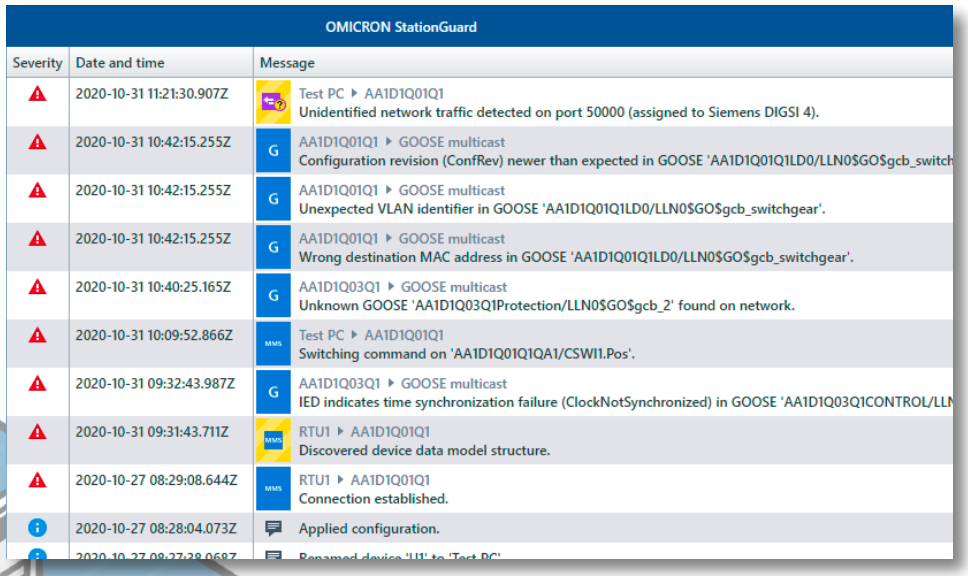
Янн Гостели (Yann Gosteli)
Начальник отдела систем автоматизации подстанций
CKW AG, Швейцария

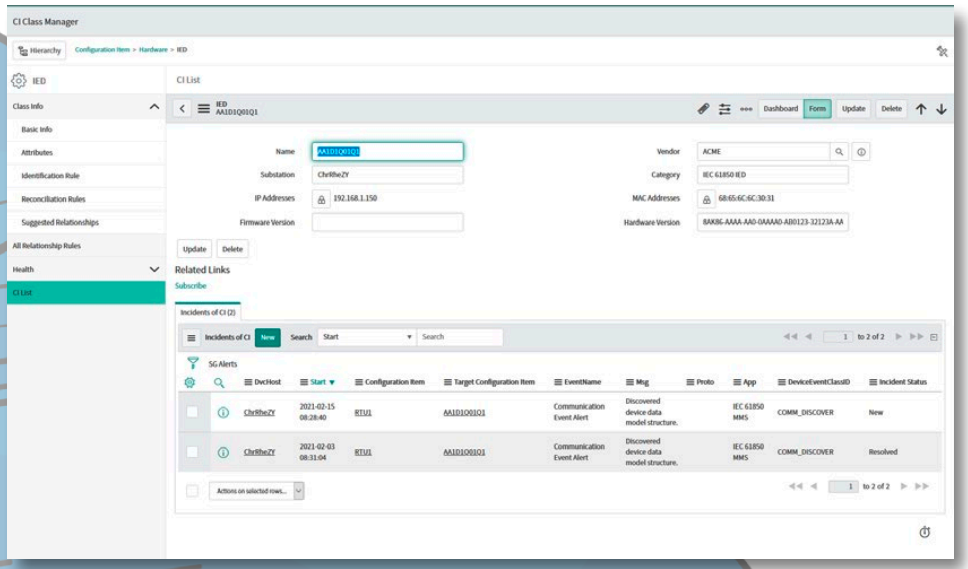
сообщениям

Журнал событий

Помимо графического представления, аварийные сигналы также записываются в журнал событий. Если пользователи вносят изменения в конфигурацию или подтверждают получение аварийных сообщений, это отображается в виде соответствующей записи. Кроме того, в журнал в хронологическом порядке вносятся записи о критических событиях, таких как операции управления, изменения режимов испытания IED и загрузка файлов (включая имена файлов).

В журнале, например, можно фильтровать все прошедшие события, связанные с определенным идентификатором. Это позволяет распознавать тенденции даже в отношении безсистемно возникающих событий.





Модуль StationGuard ServiceNow (TM)

StationGuard адаптируется к вашей стратегии ИТ-безопасности

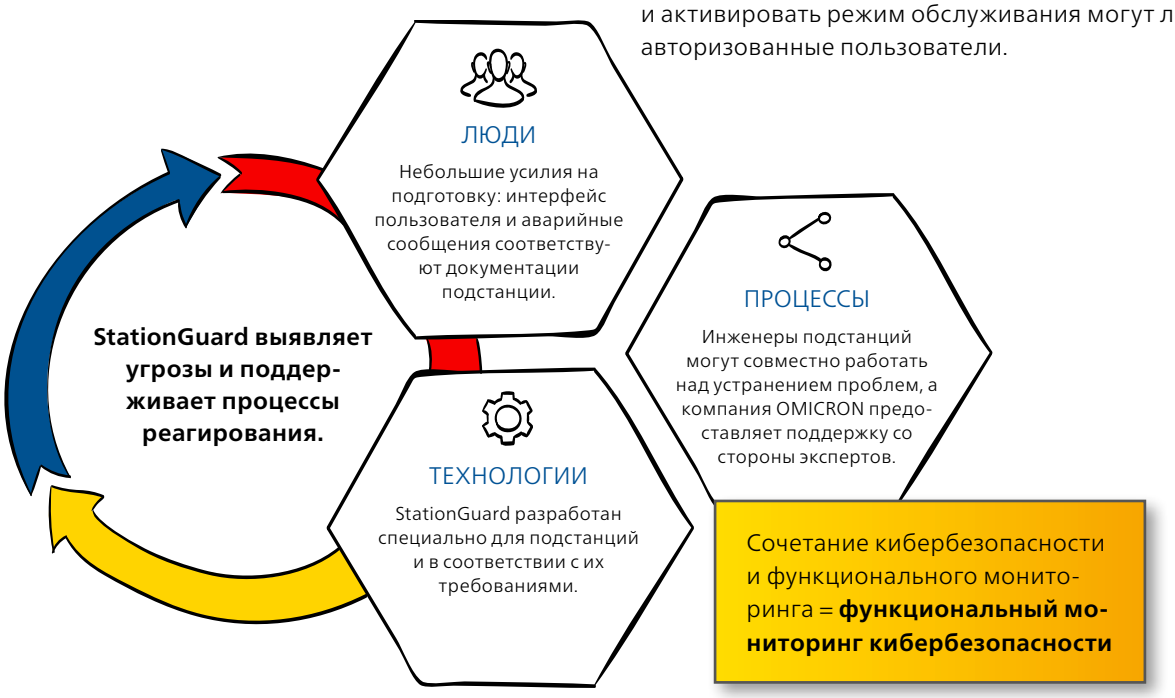
Система кибербезопасности будет эффективной только при правильном взаимодействии людей, процессов и технологий. Следовательно, один из главных вопросов звучит следующим образом: «Что происходит при получении аварийного сообщения от системы безопасности?» Цель StationGuard заключается в максимальной поддержке таких процессов реагирования с помощью современных технологий.

Ложные сигналы тревоги часто возникают, когда инженеры проводят работы на подстанции или перезагружают устройства, а также при срабатываниях релейной защиты. StationGuard содержит информацию о таких типичных событиях, а ее интерфейс адаптирован к используемым на подстанции схемам и терминологии. Это позволяет инженерам быстро определить, связано аварийное сообщение с известной операцией или же требует дальнейшего расследования.

Система визуализирует события для инженеров РЗА и выдает подробную информацию для ИТ-специалистов, что позволяет сотрудникам совместно выяснять причины тревоги.

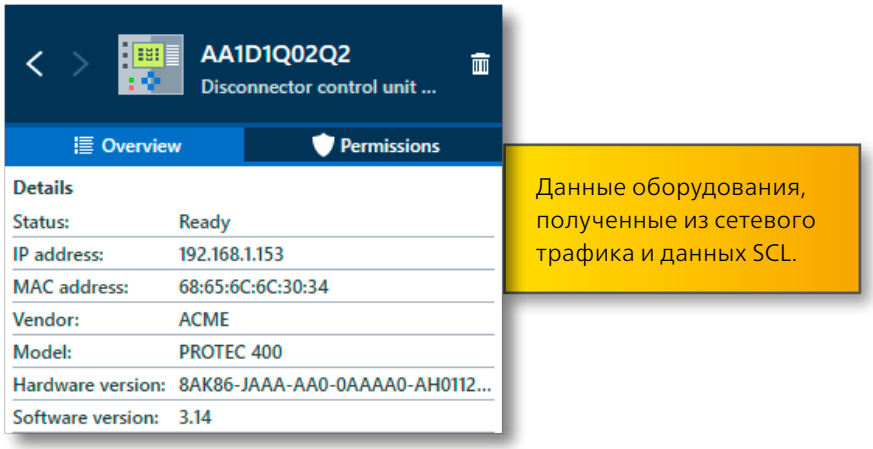
Удобная интеграция в процессы безопасности операционно-технологических (ОТ) сетей

- √ **Журнал событий**
  StationGuard записывает важные действия, такие как коммутационные операции, изменения настроек IED или квитирование аварийных сигналов.
- √ **Обнаружение и экспорт оборудования**
  Обнаруживаются все устройства, находящиеся в сети. Список оборудования может быть экспортирован. Подробная информация об оборудовании собрана из сетевого трафика и импортированных инжиниринговых файлов (SCL), включая подробные данные о версиях аппаратного и программного обеспечения.
- √ **Интеграция с SIEM и системами обработки заявок**
  С помощью протокола Syslog и наших модулей подключения StationGuard можно интегрировать со многими системами SIEM и системами обработки заявок на устранение неисправностей от разных производителей.
- √ **Трассировка сети**
  Для каждого события создается совместимая с Wireshark (PCAP) трассировка сети, на основе которой выполняется дальнейший анализ.
- √ **Аутентификация пользователя**[1]
  Интеграцию с LDAP/ActiveDirectory можно настроить в системе централизованного управления StationGuard. Вносить изменения в конфигурацию и активировать режим обслуживания могут лишь авторизованные пользователи.

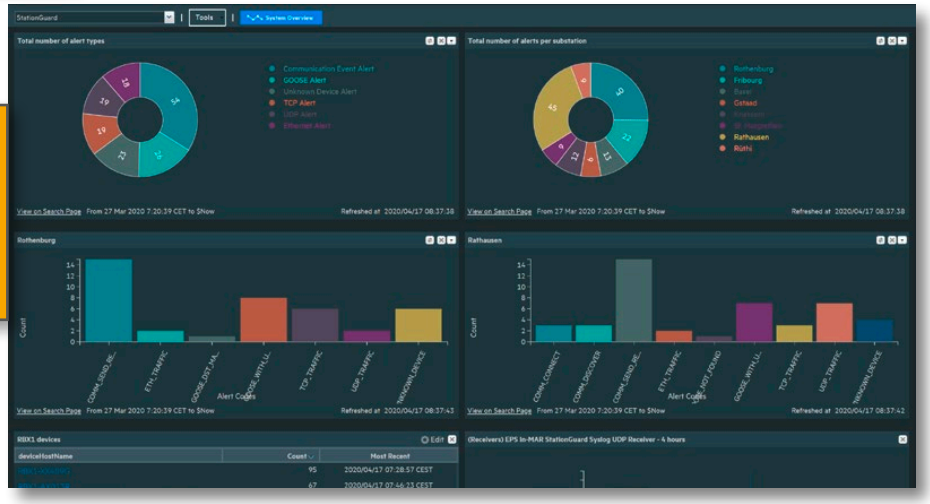


Платформа с усиленной защитой

- √ **Защищенный криптопроцессор**
  Ключи и сертификаты хранятся исключительно в чипе, защищенном от несанкционированных обращений и подделки в соответствии с ISO/IEC 11889.
- √ **Защищенная последовательность загрузки**
  Криптопроцессор используется для проверки подписей каждого загруженного программного модуля. Это гарантирует, что на устройстве может работать только программное обеспечение OMICRON.
- √ **Зашифрованные обновления с цифровой подписью**
  Устройство StationGuard принимает только обновления встроенного ПО, подписанные OMICRON. Обновления программного обеспечения для ПК также подписаны.
- √ **Безопасный производственный процесс**
  Ключи надежно хранятся на модулях аппаратной защиты; секретные ключи извлечь нельзя.
- √ **Полное шифрование диска**
  Криптопроцессор используется для шифрования всех данных с помощью уникального для каждого устройства ключа.
- √ **Специальная операционная система с усиленной защитой**
  Используется специализированная система с усиленной защитой Linux. Каждый процесс получает только те разрешения, которые необходимы для выполнения задачи.
- √ **Зашифрованная связь между устройством и ПК**
  Связь между StationGuard и ПК зашифрована по протоколу TLS (Transport Layer Security).
- √ **Наши специалисты продолжают совершенствовать систему...**
  Специалисты компании OMICRON постоянно работают над дополнительным усилением защит и усовершенствованием платформы.



Данные оборудования, полученные из сетевого трафика и данных SCL.



Анализ первопричин, предоставляемый в оповещениях StationGuard, позволяет вести статистику в SIEM любого производителя.

Три варианта платформы

Датчики StationGuard можно установить на трех различных платформах. В зависимости от потребностей систему StationGuard можно использовать на аппаратной платформе RBX1, платформе MBX1 или на виртуальной машине. Поскольку все интеллектуальные функции StationGuard заключены в датчиках, они способны работать автономно — стационарного подключения к центральному серверу не требуется.

StationGuard на платформе RBX1

StationGuard на аппаратной базе RBX1 является системой обнаружения сетевых вторжений (IDS) для защиты систем автоматизации подстанций и SCADA от киберугроз и атак нулевого дня (новейших вирусов, еще не внесенных в базы). Платформа RBX1 устанавливается в 19-дюймовую стойку для работы в сложных условиях энергосистем. У нее достаточно производительности и памяти для записи всех событий и связанного с ними трафика, даже если такое событие могло произойти очень давно.

Платформа RBX1 укомплектована уникальным набором функций безопасности, включая полное шифрование диска, микросхему криптопроцессора, совместимую с ISO/IEC 11889, и настраиваемый безопасный унифицированный расширяемый интерфейс встроенного ПО (UEFI). Также в состав платформы входят двоичные выходы для простого включения сигналов тревоги IDS в список сигналов SCADA.

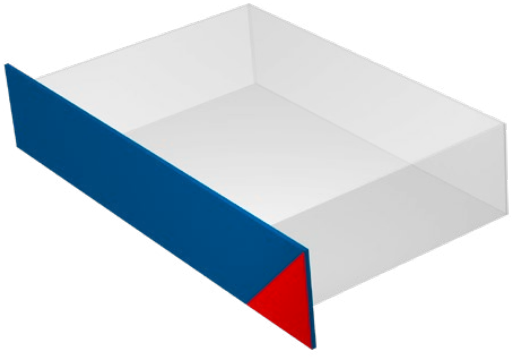
StationGuard на платформе MBX1

StationGuard на базе портативного блока оборудования MBX1 обеспечивает столь же высокий уровень безопасности, как и решение, монтируемое в стойку. Мобильная версия системы StationGuard позволяет быстро оценить безопасность подстанции или сети SCADA, а также оперативно создать инвентарный список всех устройств объекта, находящихся в сети.

На этапах ввода в эксплуатацию или технического обслуживания многие инженеры, а также внешние подрядчики подключают свое оборудование к уязвимой сети подстанции. Система StationGuard на платформе MBX1 идеально подходит для временного мониторинга сети в этот период, сигнализируя о запрещенном поведении и записывая важные действия во время ввода в эксплуатацию и технического обслуживания.

StationGuard на платформе виртуальной машины

Датчики StationGuard также доступны в виде виртуального устройства, предназначенного для установки на существующие вычислительные платформы подстанций.



Подобно системе на аппаратной платформе, виртуальная модификация также способна работать абсолютно независимо, записывая и регистрируя события даже в случае сбоя соединения с центральным сервером. Обратите внимание, что StationGuard на платформе виртуальной машины имеет некоторые технические ограничения в части функционального мониторинга шины процесса по сравнению со StationGuard на платформах RBX1 и MBX1.

Технические характеристики платформы RBX1

Условия окружающей среды

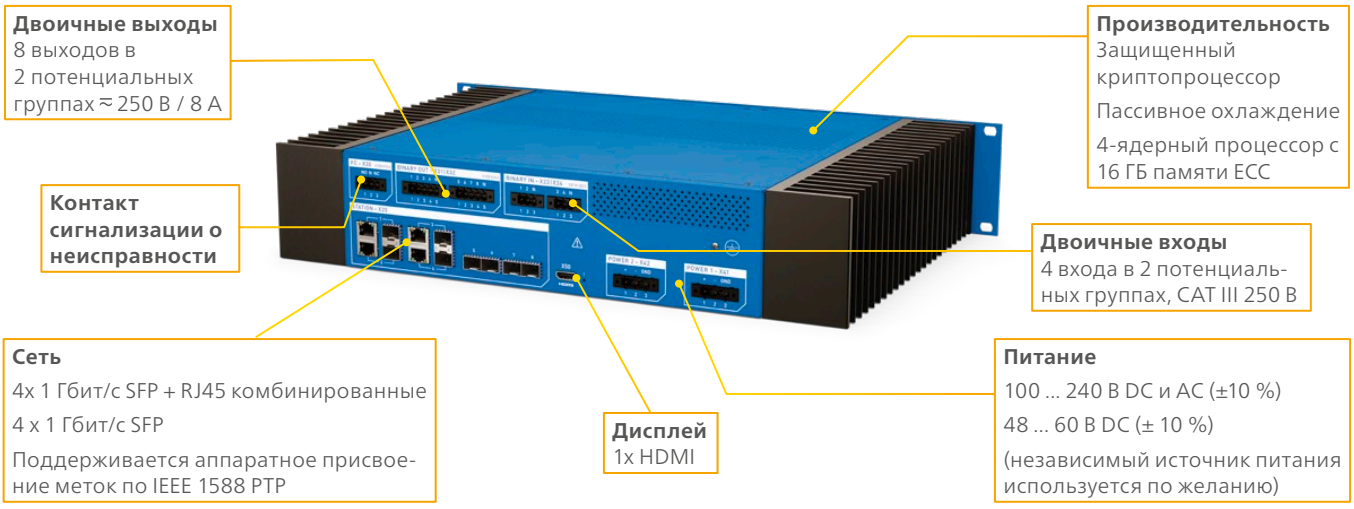
Диапазон рабочих температур	-20 ... +55 °C
Диапазон температур хранения	-25 ... +70 °C
Относительная влажность	5 ... 95 % (при отсутствии конденсации)
Защита от проникновения пыли и влаги по IEC 60529	IP30

Стандарты

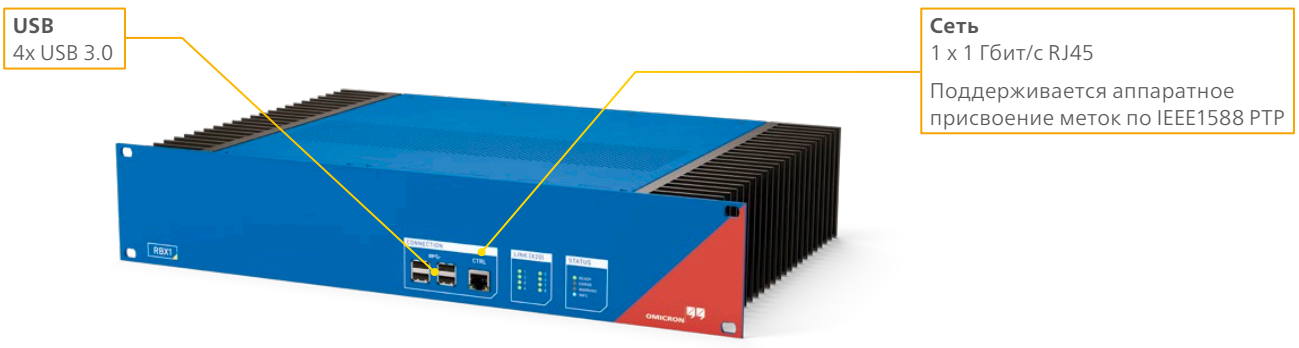
Производственные стандарты	IEC 61850-3 IEEE 1613 Уровень безопасности: Класс 1
Стандарты ЭМС	IEC 61326-1 IEC 60255-26 IEC 61000-6-5
Стандарты безопасности	EN 60255-27 EN 61010-1 EN 61010-2-030

Более подробные сведения см. в технических данных.

Платформа RBX1, вид сзади



Платформа RBX1, вид спереди



Мы предлагаем вам первоклассную киберзащиту с помощью системы StationGuard

Глубокие знания OT

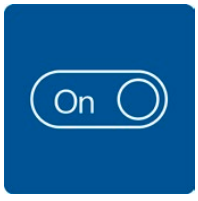
У компании OMICRON более 30 лет опыта работы в сфере операционных технологий (OT). Полученные знания были реализованы в датчиках системы StationGuard, которые предоставляют точные отчеты о любых отклонениях в работе, таких как вторжение (атака), функциональная проблема или стандартная процедура техобслуживания.

солидные знания и наработки в сфере OT

Быстрый ввод в эксплуатацию

На объектах, использующих системы IEC 61850, ввод в эксплуатацию StationGuard осуществляется мгновенно благодаря импорту файлов SCL. А на объектах с системами IEC 60870-5-104 можно существенно сократить этап настройки StationGuard, используя предустановленные роли. И в том, и в другом случае период между первым подключением системы StationGuard к сети и фактическим использованием ее возможностей будет минимальным. Кроме того, будут не нужны периоды длительной настройки, подготовки персонала и обучения.

мгновенная защита



Эффективный режим обслуживания

Режим обслуживания еще больше повышает уровень защиты. В обычном режиме работы техобслуживание запрещено и мгновенно идентифицируется системой безопасности как вторжение. При разрешенном обслуживании система StationGuard переходит в соответствующий режим и разрешает выполнение необходимых действий, обезопасив при этом все операции, в том числе выполняемые в рамках этой процедуры.

обеспечение безопасности на каждом этапе работы

Оборудование для вашей рабочей среды

Систему StationGuard можно легко интегрировать с существующей рабочей средой, используя ее возможности подключения к системам управления информацией о безопасности и событиями безопасности (SIEM), такими как ServiceNow. В устаревших системах можно через двоичные выходы с помощью проводов соединить StationGuard с центром управления безопасностью (SOC) для обеспечения оптимальной интеграции.

сотрудничество с производителями смежных систем

Максимально глубокий анализ пакетов

Система регистрации записей StationGuard отлично подходит для анализа определенного поведения (на протяжении длительного времени), а возможности Wireshark PCAP позволяют аналитикам тщательно изучить подозрительные пакеты на уровне бита.

постоянный мониторинг обмена данными

Всесторонняя поддержка

Поддержка от экспертов StationGuard

Если аварийное сообщение указывает на несанкционированное или нестандартное поведение ПК или устройств на объекте, специалисты StationGuard могут предложить поддержку в анализе ситуации. Они просмотрят записи параметров сети и, зная процедуры обмена данными и уязвимости каждого устройства, определят, может ли это событие представлять угрозу или оно было вызвано технической проблемой.

Обращайтесь в нашу службу технической поддержки, которая после безопасной передачи данных о событии свяжется с экспертом в одном из офисов OMICRON. Наши специалисты осведомлены об особенностях надлежащей работы коммуникационных устройств, а также об уязвимостях устройств защиты, автоматизации и управления такого оборудования практически всех мировых производителей.

«Как эксперт по уязвимостям безопасности в IED, я точно знаю, как выявить сетевую атаку. И вам в этом с удовольствием помогу!»

Стефан Лассьер (Stefan Lässer),
специалист по уязвимостям IED IEC 61850

«Я вхожу в ряд рабочих групп по стандартизации и опубликовал множество статей о коммуникации на подстанциях, поэтому ко мне часто обращаются электроэнергетические компании с просьбой помочь в решении запутанных проблем с GOOSE, Sampled Values и MMS».

Фред Штейнхаузер (Fred Steinhauser)
эксперт по цифровым подстанциям

Техническая поддержка 24/7

Обратившись в службу технической поддержки, вы быстро получите помощь наших квалифицированных технических специалистов. Мы работаем 24 часа в сутки, 7 дней в неделю.

У нас есть все основания гордиться своим качеством продукции и уровнем обслуживания!

«Я работаю в службе технической поддержки OMICRON с 2010 года и специализируюсь на системах IEC 61850».

Лукас Гасснер (Lukas Gassner),
специалист службы технической поддержки OMICRON

24 7 support

Мы предлагаем нашим клиентам только лучшее...

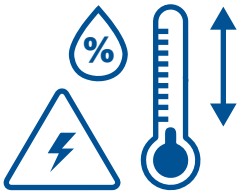
Качество

Вы всегда можете быть уверены в высоких стандартах безопасности

Максимальная надежность:

72

часа отбраковочных испытаний перед поставкой



Более

30.000

автоматически выполненных испытаний в режиме 24/7

ISO 9001
TÜV & EMAS
ISO 14001
OHSAS 18001

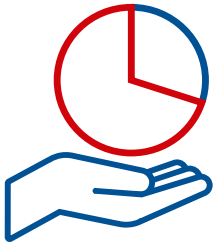
Соответствие международным стандартам

Инновации

Экономия до

70%

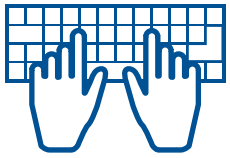
времени при установке и в работе

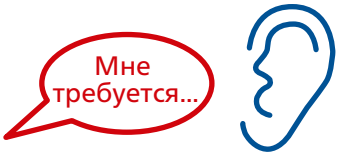


Более

200

разработчиков постоянно совершенствуют решения





...продукция, соответствующая моим требованиям

Более

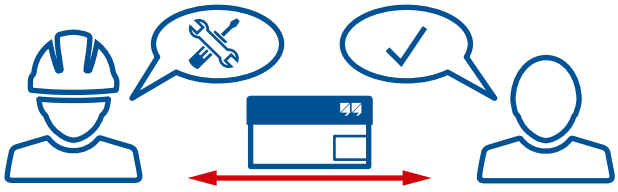
15%

годового оборота инвестируется в исследования и разработки

Поддержка

Круглосуточная профессиональная техподдержка

представительств по всему миру



Рентабельность и простота обслуживания

Простой и быстрый процесс предоставления готовых решений экспертами по кибербезопасности

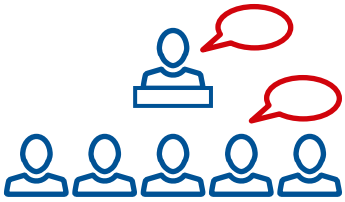
Знания

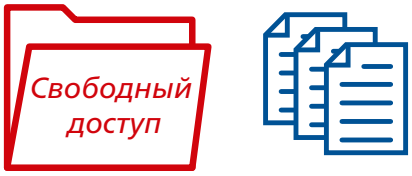
Более

300

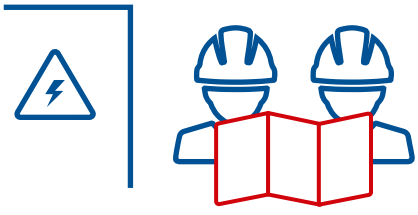
учебных курсов и множество практических тренингов на протяжении года

Встречи пользователей, семинары и конференции, часто проводимые компанией OMICRON





...к тысячам пособий и указаний по применению



Огромный опыт в сфере консультирования и помощи со вводом оборудования в эксплуатацию

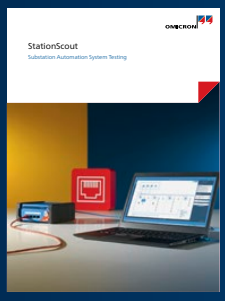
OMICRON — международная компания, видящая своей главной целью идею сделать системы электроснабжения надежными и безопасными. Наши новаторские разработки созданы для решения сегодняшних и будущих вызовов в электроэнергетике. Мы всегда делаем ещё больше для наших пользователей: оперативно реагируем на потребности, обеспечиваем высококачественную поддержку на местах и делимся своими знаниями и наработками.

Опытные специалисты OMICRON проводят исследования и разрабатывают инновационные технологии для всех областей электроэнергетики. Пользователи со всего мира полагаются на точность, качество и быстродействие наших удобных современных решений для испытания оборудования высокого и среднего напряжения, проверки устройств защиты, испытания цифровых подстанций и обеспечения кибербезопасности.

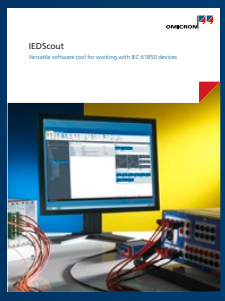
С момента основания в 1984 году компания OMICRON накопила значительный опыт в области электроэнергетики. Команда из более 900 специалистов в 25 офисах по всему миру обеспечивает поддержку наших продуктов в режиме «24/7» для клиентов из более чем 160 стран.

В следующих публикациях содержится дополнительная информация об устройствах, описанных в данном каталоге и о других вспомогательных устройствах:

Брошюра
IEC 61850



Брошюра
StationScout



Брошюра
IEDScout

Брошюра
DANEO 400

Более подробную информацию, дополнительную литературу и подробную контактную информацию наших региональных офисов по всему миру вы можете найти на нашем веб-сайте.

www.omicronenergy.com

L4300