

БЕЗОПАСНОСТЬ АСУ ТП ИТОГИ 2017 ГОДА



СОДЕРЖАНИЕ

Введение.....	3
Список сокращений.....	3
Анализ уязвимостей компонентов АСУ ТП.....	4
Распространенность компонентов АСУ ТП в сети Интернет.....	7
Заключение.....	12

ВВЕДЕНИЕ

В последние годы хакеры все чаще атакуют промышленность, энергетику, транспорт. Крупные финансовые потери судоходной компании Maersk, остановка заводов Renault Nissan, взлом системы общественного транспорта Сан-Франциско, диверсии в отношении энергетических предприятий с использованием ПО BlackEnergy и Industroyer/CrashOverride — вот лишь несколько недавних печальных примеров.

Информационная безопасность критически важных объектов неразрывно связана с защищенностью АСУ ТП (ICS). Казалось бы, в этой области проделана немалая работа — государственные органы в разных странах совершенствуют законодательную базу, центры реагирования на компьютерные инциденты (CERT) выпускают бюллетени и все больше вендоров АСУ ТП понимают, что уязвимости их продуктов могут стать причиной срыва крупного контракта¹ или даже привести к человеческим жертвам.

Однако несмотря на ощутимые финансовые потери в ходе многочисленных инцидентов и растущий интерес к практической безопасности состояние защищенности большинства объектов промышленности со времен атаки Stuxnet (с 2010 года) почти не изменилось, что и подтверждается данным отчетом.

Проблема может усугубиться повсеместным подключением АСУ ТП к глобальным сетям, которое ожидается с приходом четвертой индустриальной революции. В таких условиях вполне возможен перехват управлением технологическим процессом из любой точки земного шара без непосредственного физического доступа.

Сегодня практически любой продвинутый пользователь интернета с помощью общедоступных поисковых систем может обнаружить в сети IP-адреса компонентов промышленного сетевого оборудования (коммутаторов, конвертеров интерфейсов, шлюзов и т. п.). И если злоумышленники получают контроль над такими устройствами, это может нарушить функционирование инженерных систем зданий или производственной инфраструктуры. В 2017 году мы зафиксировали увеличение доли уязвимостей такого оборудования².

Данное исследование, уже четвертое по счету, содержит результаты анализа уязвимостей компонентов АСУ ТП и их распространенности в сети Интернет и позволяет оценить ситуацию в динамике за последние несколько лет.

СПИСОК СОКРАЩЕНИЙ

RTU — remote terminal unit

SCADA — supervisory control and data acquisition

АСУ ТП — автоматизированная система управления технологическим процессом

ЛВС — локальная вычислительная сеть

ПЛК — программируемый логический контроллер

ПО — программное обеспечение

РСУ — распределенные системы управления

ТУД — терминал удаленного доступа и управления

ЧМИ — человеко-машинный интерфейс

¹ В декабре 2017 года «Транснефть» объявила, что больше не будет использовать оборудование производства Schneider Electric из-за многочисленных уязвимостей, ставящих под угрозу кибербезопасность компании.

² Примеры атак с использованием сетевого оборудования будут описаны в нашем отдельном исследовании; следите за новостями на сайте ptsecurity.com.

АНАЛИЗ УЯЗВИМОСТЕЙ КОМПОНЕНТОВ АСУ ТП

Методика исследования уязвимостей

В качестве основы для исследования была использована информация из общедоступных источников, таких как базы знаний уязвимостей, уведомления производителей, сборники эксплойтов, доклады научных конференций, публикации на специализированных сайтах и в блогах³.

В качестве базы знаний уязвимостей использовались следующие ресурсы:

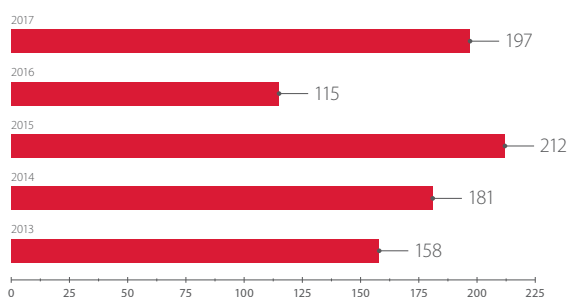
- + ICS-CERT (ics-cert.us-cert.gov);
- + NVD (nvd.nist.gov), CVE (cve.mitre.org);
- + Positive Research Center (securitylab.ru/lab);
- + Siemens Product CERT (siemens.com/cert);
- + Schneider Electric Cybersecurity Support Portal⁴.

Степень риска уязвимостей компонентов АСУ ТП определяется на основе значения Common Vulnerability Scoring System (CVSS) третьей версии (first.org/cvss).

Динамика обнаружения уязвимостей

При анализе опубликованных уязвимостей был использован ограниченный список, в который вошли крупные и наиболее известные производители оборудования, используемого в промышленной автоматизации.

По сравнению с 2016 годом количество новых опубликованных уязвимостей выросло: на момент подготовки исследования была обнародована информация о 197 уязвимостях основных производителей. Следует отметить, что данные по некоторым уязвимостям могут быть опубликованы позже, после их устранения: это определяется политикой ответственного разглашения. Например, 30 уязвимостей оборудования компании Муха, обнаруженные в 2016 году, были опубликованы только в 2017 году.



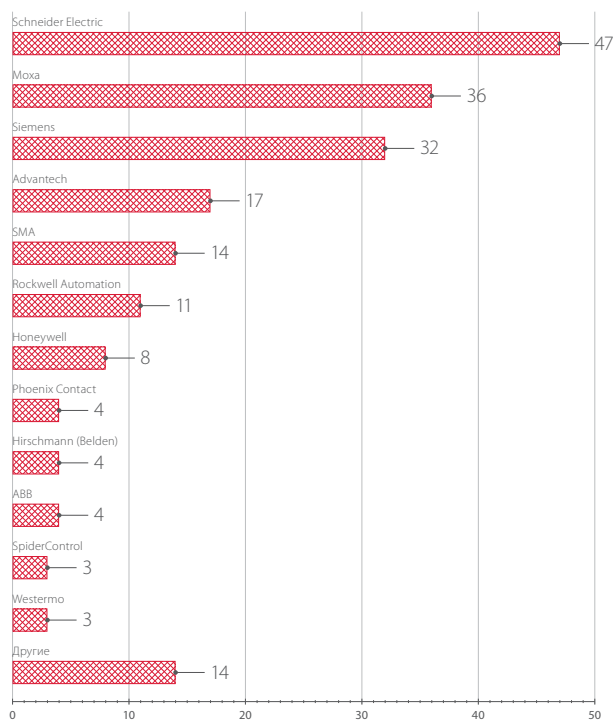
Общее количество уязвимостей, обнаруженных в компонентах АСУ ТП

Количество опубликованных в 2017 году уязвимостей по производителям

По сравнению с 2016 годом лидеры поменялись. Первую позицию вместо компании Siemens теперь занимает Schneider Electric. В 2017 году было опубликовано почти в десять раз больше уязвимостей (47), связанных с компонентами этого вендора, нежели годом ранее (5). Также следует обратить внимание на количество новых недостатков безопасности в промышленном сетевом оборудовании Муха — их было опубликовано вдвое больше (36), чем в прошлом году (18).

³ digitalbond.com, scadahacker.com, immunityinc.com/products/canvas, exploit-db.com, rapid7.com/db

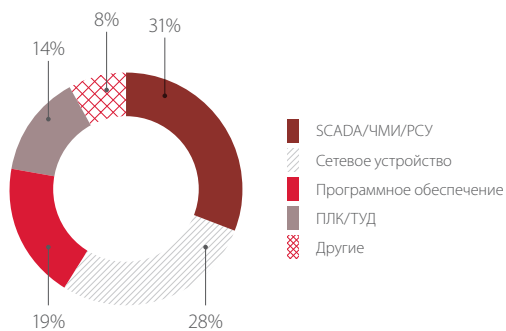
⁴ schneider-electric.com/b2b/en/support/cybersecurity/report-an-incident.jsp



Количество опубликованных в 2017 году уязвимостей
по основным производителям компонентов АСУ ТП

Уязвимости по компонентам

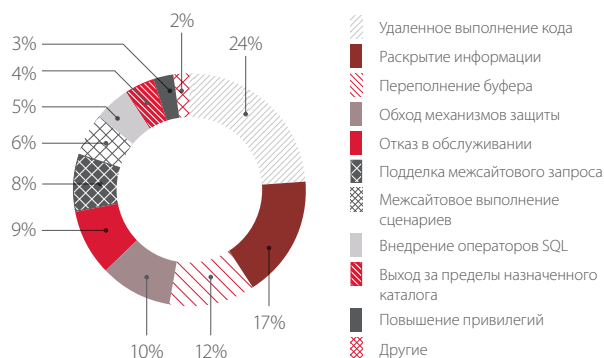
Основной тренд — рост числа новых уязвимостей в промышленном сетевом оборудовании. Недостатки безопасности были выявлены в продукции Moxa (36), Hirschmann (4) и Phoenix Contact (4). Если в 2016 году в сетевых устройствах было разглашено в полтора раза меньше уязвимостей, чем в компонентах SCADA/ЧМИ/PCУ⁵, то по итогам минувших 12 месяцев разрыв сократился до минимума.



Доля новых уязвимостей в различных компонентах АСУ ТП

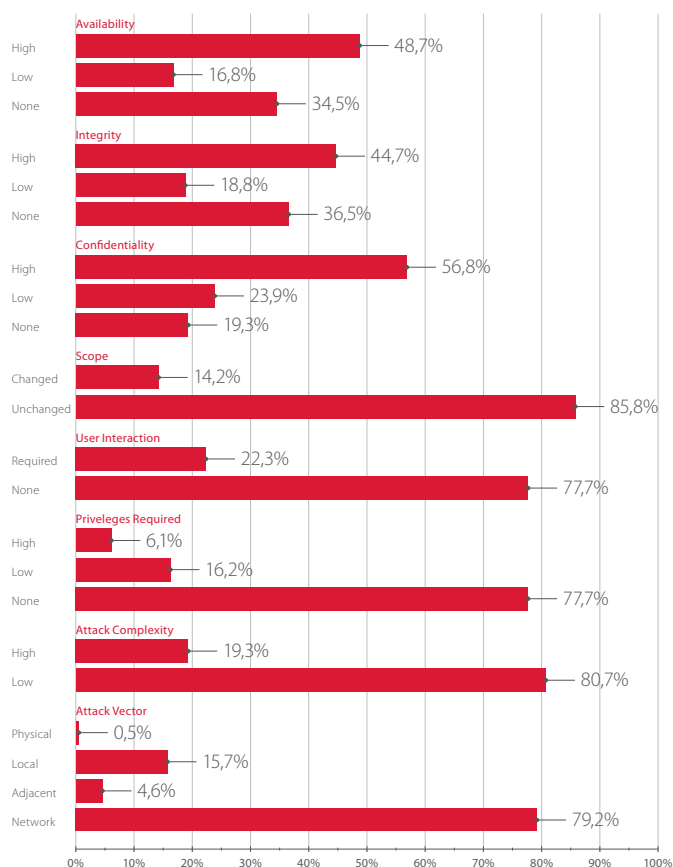
⁵ Компоненты АСУ ТП для диспетчеризации и мониторинга.

К наиболее распространенным типами уязвимостей относятся «Раскрытие информации», «Удаленное выполнение кода» и «Переполнение буфера». В 2016 году два лидера были теми же, а на третьем месте находились уязвимости типа «Отказ в обслуживании».



Распространенные типы уязвимостей компонентов АСУ ТП

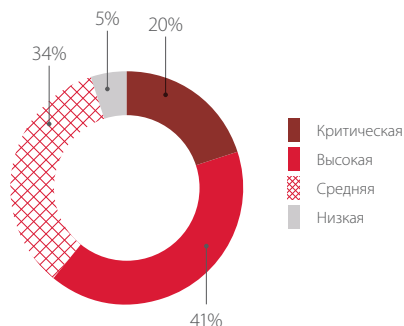
Распределение по метрикам CVSS версии 3 по сравнению с 2016 годом практически не изменилось. Большинство обнаруженных в этом году уязвимостей могут эксплуатироваться удаленно без необходимости предварительного получения каких-либо привилегий.



Распределение уязвимостей в соответствии со значениями метрик CVSS

Степень риска выявленных уязвимостей

Большее половины выявленных уязвимостей относятся к критической и высокой степени риска в соответствии с оценкой CVSS версии 3. При этом доля уязвимостей критической степени риска выросла на 3% по сравнению с предыдущим годом.



Распределение уязвимостей по степеням риска

РАСПРОСТРАНЕННОСТЬ КОМПОНЕНТОВ АСУ ТП В СЕТИ ИНТЕРНЕТ

Методика исследования

Сбор данных о доступности компонентов АСУ ТП в сети Интернет осуществлялся исключительно пассивными методами. Использовались результаты сканирования портов ресурсов, доступных в сети Интернет, которые были получены с помощью общедоступных поисковых систем — Google, Shodan (shodan.io), Censys (censys.io).

При использовании пассивных методов сбора данных о доступности компонентов АСУ ТП в сети Интернет были выявлены некоторые ограничения:

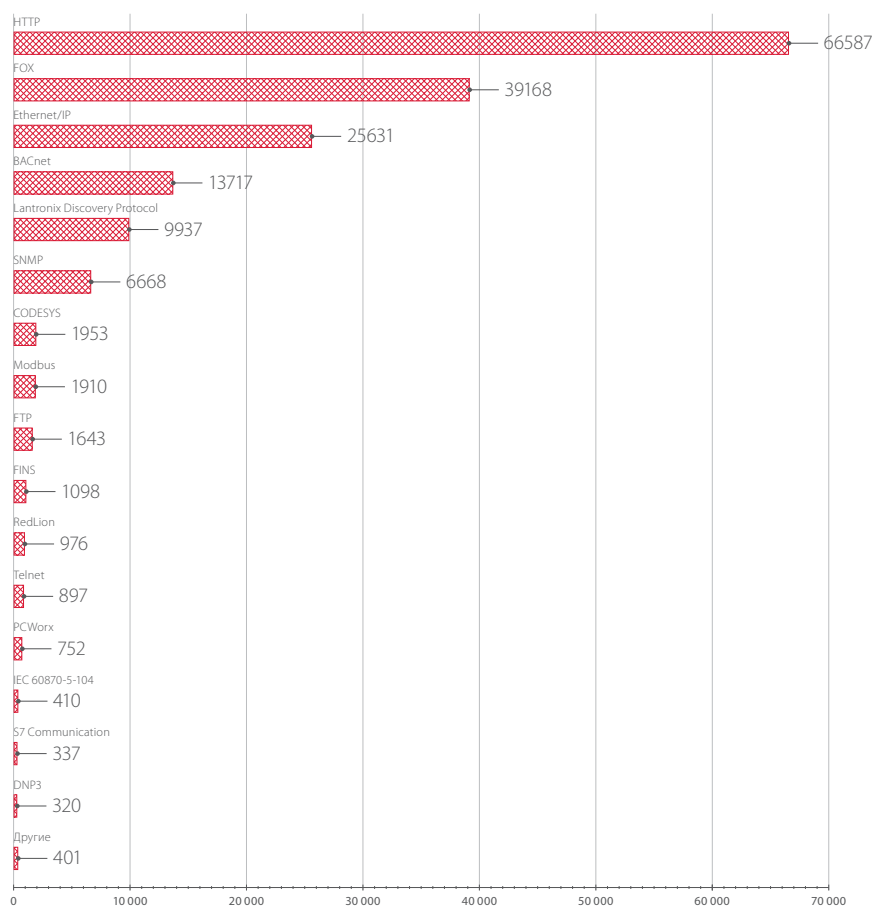
- + Сервис Shodan сканирует ограниченное число портов и производит сканирование сети Интернет с определенных IP-адресов, которые вносятся некоторыми администраторами и производителями сетевых экранов в черные списки. Поэтому для расширения области анализа использовались данные, полученные с помощью поисковых систем Google и Censys.
- + Определение версий используемых продуктов зачастую не представлялось возможным по причине отсутствия данных о них в баннерах (т. е. в текстах, отображаемых исследуемыми хост-серверами).

После получения информации из общедоступных источников был проведен ее дополнительный анализ на предмет взаимосвязи с АСУ ТП. Специалисты Positive Technologies составили базу данных идентификаторов АСУ ТП, которая позволяет на основе баннера сделать заключение об используемом продукте и его производителе.

Распространенность

В результате исследования всего было выявлено 175 632 компонента АСУ ТП, доступных в сети Интернет.

Если рассматривать доступные компоненты в зависимости от используемого ими протокола, то наибольшее количество компонентов АСУ ТП, как и в прошлые годы, доступно по протоколу HTTP. Также широко распространен протокол Fox, используемый в продуктах Niagara Framework: он предназначен преимущественно для автоматизации зданий, сооружений, дата-центров. Подобные системы управляют кондиционированием, энергоснабжением, телекоммуникациями, сигнализацией, освещением, камерами видеонаблюдения и другими ключевыми инженерными элементами, часто содержат уязвимости⁶ и уже подвергались взлому⁷.



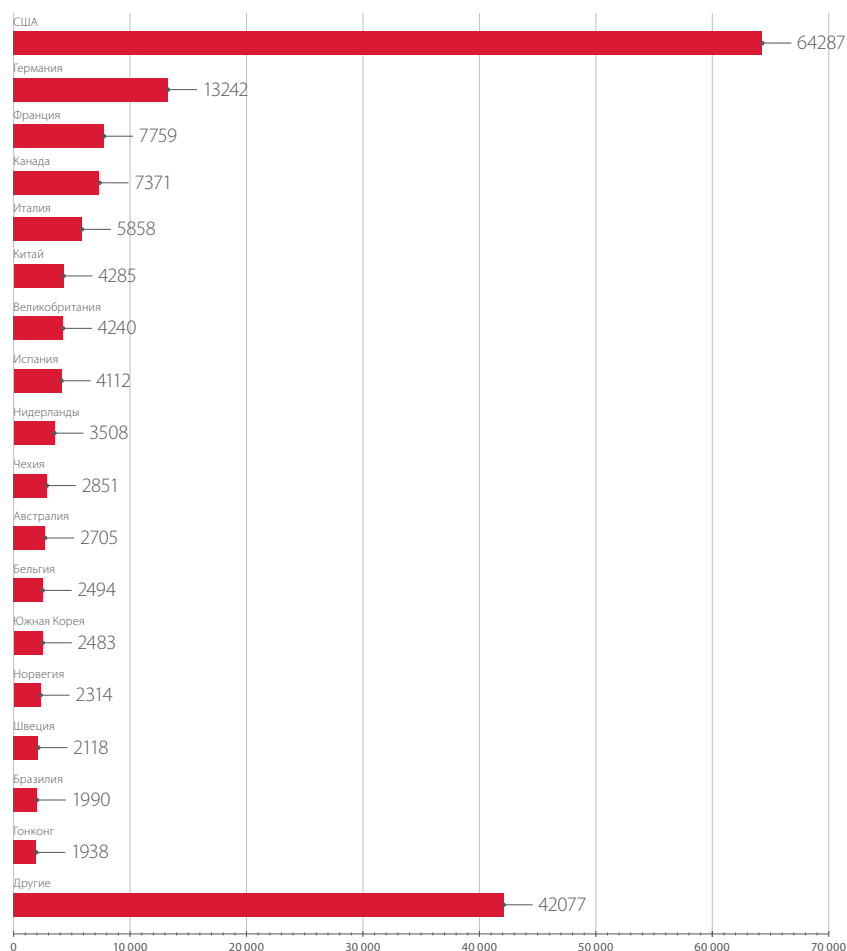
Количество компонентов АСУ ТП, доступных в сети Интернет
(распределение по используемым протоколам)

⁶ ics-cert.us-cert.gov/advisories/ICSA-12-228-01A

⁷ info.publicintelligence.net/FBI-Antisec/ICS.pdf

Территориальное распределение

Лидером по количеству найденных компонентов с большим отрывом уже не первый год является США, при этом их доля возросла почти на 10% и теперь составляет примерно 42% от общего числа найденных компонентов. Второе место, как и в прошлом году, занимает Германия (6%). Далее расположилась Франция (5%), а Китай с третьего места переместился на шестое.



Интересный факт

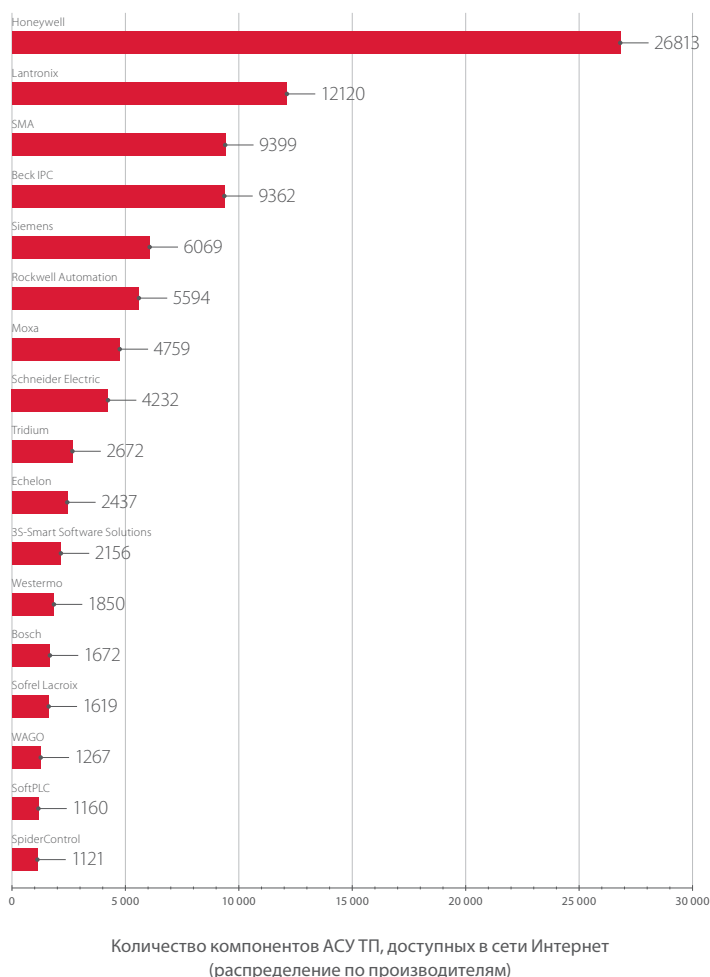
Россия в этом году поднялась на три позиции и занимает 28-е место. В 2016 году в России был обнаружен 591 компонент АСУ ТП, а в 2017 году — 892. Можно говорить о растущей угрозе, связанной с увеличением доступных из интернета компонентов АСУ ТП, расположенных в России.

Количество компонентов АСУ ТП, доступных в сети Интернет
(распределение по странам)

Распространенность по производителям и продуктам

На первом месте — компания Honeywell, которая является владельцем компании Tridium и продукта Niagara Framework. Следует отметить, что часть других продуктов серии Niagara остались под старой маркой, поэтому Tridium отдельно присутствует в отчете.

Второе место в этом году заняла Lantronix. Это калифорнийская компания — производитель устройств для удаленного доступа к оборудованию через интернет.



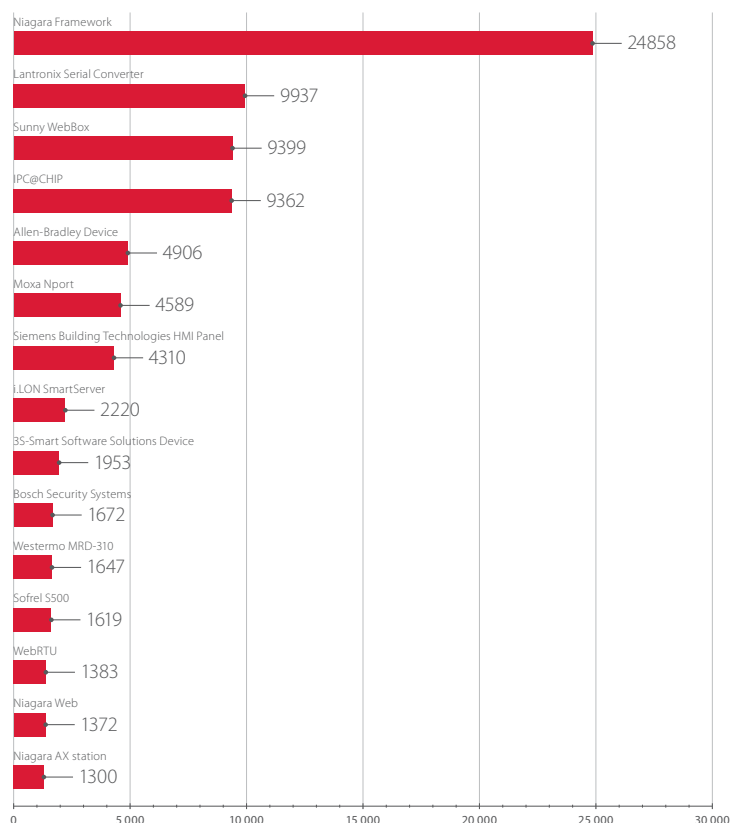
Согласно недавнему исследованию⁸, в интернете доступно несколько тысяч конвертеров интерфейсов производства Lantronix, и почти половина этих устройств раскрывает свои пароли для подключения по протоколу Telnet. Это подтверждаются и нашим исследованием: мы обнаружили в общей сложности 12 120 доступных устройств Lantronix, в том числе и уязвимых.

Доступность таких устройств, несмотря на их вспомогательную роль, представляет большую опасность для технологического процесса. Конвертеры интерфейсов необходимы для связи компонентов АСУ ТП друг с другом и нарушение их работы может вызвать потерю удаленного контроля и управления. Например, в ходе кибератаки на энергосистему Украины⁹ злоумышленники удаленно вывели из строя конвертеры компании Мохы, в результате чего была потеряна связь с полевыми устройствами на электроподстанциях. Это привело к потере возможности удаленного управления коммутационным оборудованием подстанций.

Программный продукт Niagara Framework по-прежнему лидирует по количеству доступного в интернете оборудования. Помимо конвертеров сетевых интерфейсов компании Lantronix, которые в этом году вышли на второе место, лидирующие позиции также заняли конвертеры компании Мохы.

⁸ bleepingcomputer.com/news/security/thousands-of-serial-to-ethernet-devices-leak-telnet-passwords/

⁹ boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf



Количество компонентов АСУ ТП, доступных в сети Интернет
(распределение по продуктам)



Типы компонентов АСУ ТП

Распределение доступных в интернете компонентов по типам в этом году практически не изменилось. Единственное отличие по сравнению с предыдущим годом — значительное увеличение доли сетевых устройств.

Соотношение типов компонентов АСУ ТП, доступных в сети Интернет

Тип компонента АСУ ТП	Доля в 2017 году	Доля в 2016 году
SCADA/PCY/ЧМИ и (или) ПЛК/ТУД (RTU) ¹⁰	14,2%	13,6%
ПЛК/ТУД (RTU)	13,2%	12,9%
Сетевое устройство	12,9%	5,1%
SCADA/PCY/ЧМИ	7,1%	7,8%
Электроизмерительный прибор	6,3%	5,2%
Другие компоненты	46,5%	55,5%

¹⁰ В эту группу вошли элементы, которые нельзя однозначно отнести к определенному типу. Например, такие многофункциональные продукты, как Niagara Framework.



ЗАКЛЮЧЕНИЕ

По итогам 2017 года отмечается увеличение количества уязвимостей, опубликованных основными производителями компонентов АСУ ТП. При этом больше половины уязвимостей имеют критическую и высокую степень риска.

Количество компонентов АСУ ТП, доступных в сети Интернет, увеличивается с каждым годом. Наибольшее их число обнаружено в странах, в которых системы автоматизации развиты лучше всего (США, Германия, Франция, Канада, Италия, Китай).

Рост количества известных уязвимостей, а также доступных в интернете компонентов АСУ ТП дает злоумышленникам все больше возможностей для проведения атак, что может привести к серьезным последствиям. Для реагирования на сложные атаки в сфере АСУ ТП необходима большая заблаговременная подготовительная работа. Еще на этапе проектирования АСУ ТП разработчики должны предусматривать механизмы безопасности, предназначенные для защиты компонентов АСУ ТП от нарушителей.

Для выявления потенциальных векторов атак и создания эффективной системы защиты промышленные предприятия должны проводить регулярный анализ защищенности АСУ ТП, а также использовать специализированные системы управления инцидентами кибербезопасности АСУ ТП.

Также необходимо применять базовые принципы обеспечения информационной безопасности:

- + отделять технологическую сеть АСУ ТП от корпоративной ЛВС и внешних сетей;
- + ограничивать физический доступ к сетям и компонентам АСУ ТП;
- + использовать строгую парольную политику;
- + контролировать параметры сетевого оборудования и правила фильтрации трафика на межсетевых экранах;
- + защищать привилегированные учетные записи;
- + минимизировать привилегии пользователей и служб;
- + использовать антивирусное программное обеспечение;
- + регулярно обновлять ПО, устанавливать обновления безопасности ОС.

О компании

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