

A low-angle, upward-looking photograph of a large industrial plant. On the left, a tall, segmented metal smokestack rises towards the sky. To the right, a complex network of metal pipes, walkways, and structural beams forms a multi-level framework. The scene is bathed in a warm, orange-gold light, suggesting a sunrise or sunset, with the sun's glow visible in the center of the frame. The sky is a pale blue with some light clouds.

POSITIVE TECHNOLOGIES

Уязвимости в АСУ ТП: итоги 2018 года

Содержание

Введение.....	2
Список сокращений.....	2
Анализ уязвимостей компонентов АСУ ТП.....	3
Методика исследования уязвимостей.....	3
Динамика обнаружения уязвимостей.....	3
Распределение опубликованных в 2018 году уязвимостей по производителям.....	4
Распределение уязвимостей по компонентам.....	4
Распределение уязвимостей по типу.....	5
Распределение уязвимостей по их воздействию.....	5
Распределение уязвимостей по степени риска.....	6
Краткие сведения об уязвимостях в компонентах АСУ ТП, выявленных специалистами Positive Technologies.....	6
Распространенность компонентов АСУ ТП в интернете.....	7
Методика исследования.....	7
Распространенность.....	7
Территориальное распределение.....	8
Распределение по производителям и продуктам.....	8
Типы компонентов АСУ ТП.....	8
Заключение.....	9

Введение

2018 год оказался богат на инциденты в сфере АСУ ТП. Были опубликованы подробности атаки с использованием кибероружия Triton, аналога Stuxnet и Industroyer, который нацелен на оборудование АСУ ТП. Кроме того, произошло несколько довольно громких инцидентов в промышленных компаниях, в частности Boeing заявил об атаке WannaCry, а спустя несколько месяцев тот же вирус стал причиной приостановки заводов Taiwan Semiconductor Manufacturing Company. Хотя эти атаки были нацелены на IT-инфраструктуру, их последствия негативно отразились и на производстве. Получается, что злоумышленнику не всегда нужно обладать какими-то специальными знаниями о технологическом процессе, чтобы повлиять на него.

После успешной эксплуатации уязвимостей в IT-инфраструктуре появляется возможность доступа к технологическому сегменту. Согласно нашим исследованиям, 82% промышленных организаций не готовы противостоять внутреннему нарушителю, который стремится проникнуть в технологическую сеть из корпоративной. А после получения доступа к технологическому сегменту сети у злоумышленника появляются широкие возможности по злонамеренному влиянию на компоненты АСУ ТП, и самый распространенный путь — это эксплуатация известных уязвимостей. Поэтому так важно знать об уязвимостях, имеющихся в оборудовании АСУ ТП: это позволяет владельцу вовремя оценивать возможные риски и принимать адекватные защитные меры.

Данное исследование содержит информацию об известных уязвимостях в компонентах АСУ ТП и их распространенности в интернете и позволяет оценить ситуацию в динамике за последние несколько лет.

Список сокращений

SCADA	supervisory control and data acquisition (диспетчерское управление и сбор данных)
АРМ	автоматизированное рабочее место
АСУ ТП	автоматизированная система управления технологическим процессом
ПЛК	программируемый логический контроллер
ТУД	терминал удаленного доступа
ПО	программное обеспечение
РСУ	распределенные системы управления
ЧМИ	человеко-машинный интерфейс

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, доклады на конференциях, публикации на специализированных сайтах и в блогах.

В качестве базы знаний уязвимостей использовались следующие ресурсы:

- ICS-CERT (ics-cert.us-cert.gov);
- NVD (nvd.nist.gov), CVE (cve.mitre.org);
- Исследовательский центр Positive Research (securitylab.ru/lab).

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

В данное исследование попадают уязвимости, информация о которых была опубликована в 2018 году; также в нем содержатся дополнительные сведения об уязвимостях, найденных нашими экспертами в 2018 году, информация о которых была опубликована уже в 2019-м.

При анализе информации об опубликованных уязвимостях рассматривались уязвимости, найденные в оборудовании наиболее известных производителей компонентов для АСУ ТП.

Динамика обнаружения уязвимостей

По сравнению с 2017 годом количество новых уязвимостей в компонентах АСУ ТП выросло на 30%: на момент подготовки исследования опубликована полная информация о 243 уязвимостях, и еще 14 находятся на стадии анализа.

Зачастую в результате детального исследования той или иной системы обнаруживается не одна, а несколько уязвимостей. Например, при анализе системы управления процессами APROL компании B&R Automation¹ наши специалисты нашли [12 уязвимостей](#).

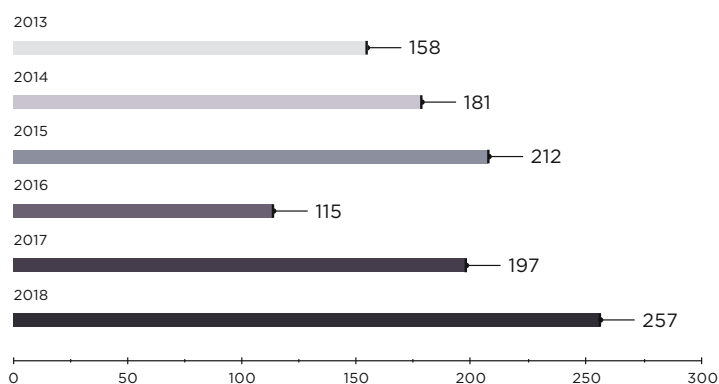


Рисунок 1. Общее количество уязвимостей,
обнаруженных в компонентах АСУ ТП

1. С июля 2017 года входит в состав компании ABB, одного из мировых лидеров по производству промышленного оборудования.

Распределение опубликованных в 2018 году уязвимостей по производителям

В 2018 году лидером по количеству новых уязвимостей все так же остается компания Schneider Electric — даже несмотря на то, что количество вновь обнаруженных уязвимостей в оборудовании производства Siemens возросло почти в два раза. Подобное лидерство этих двух компаний вполне объяснимо: популярные производители имеют широкие линейки продуктов, используемых повсеместно.

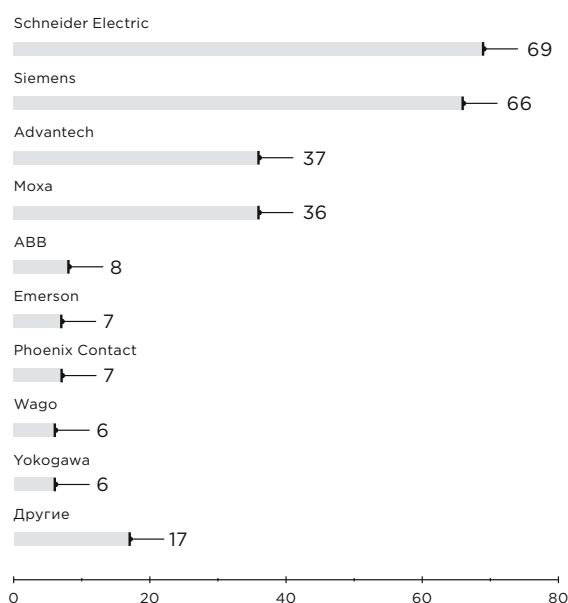


Рисунок 2. Распределение опубликованных в 2018 году уязвимостей по основным производителям компонентов АСУ ТП

Распределение уязвимостей по компонентам

В 2018 году распределение уязвимостей по компонентам АСУ ТП заметно изменилось. Если в 2017 году большая доля уязвимостей приходилась на такие компоненты, как SCADA/ЧМИ, то в 2018 году распределение уязвимостей между SCADA/ЧМИ, ПЛК/ТУД и промышленным сетевым оборудованием — практически одинаково.

По сравнению с предыдущим годом доля уязвимостей в компонентах ПЛК/ТУД выросла на 7%. Стоит отметить, что наши эксперты обнаружили 10 уязвимостей в модулях ПЛК компаний Siemens и Schneider Electric.

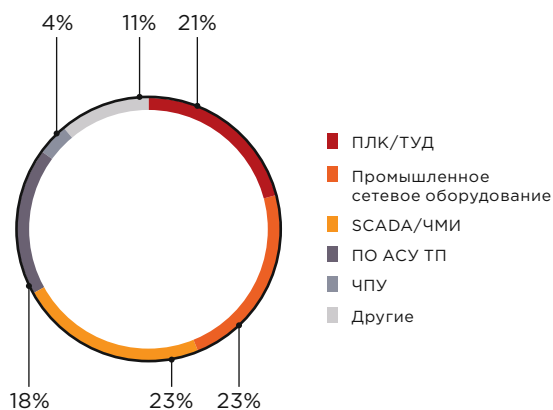


Рисунок 3. Доли уязвимостей, найденных в различных компонентах АСУ ТП

Распределение уязвимостей по типу

Значительная доля уязвимостей связана с некорректной аутентификацией или избыточными правами. При этом больше половины этих уязвимостей (64%) могут эксплуатироваться удаленно.

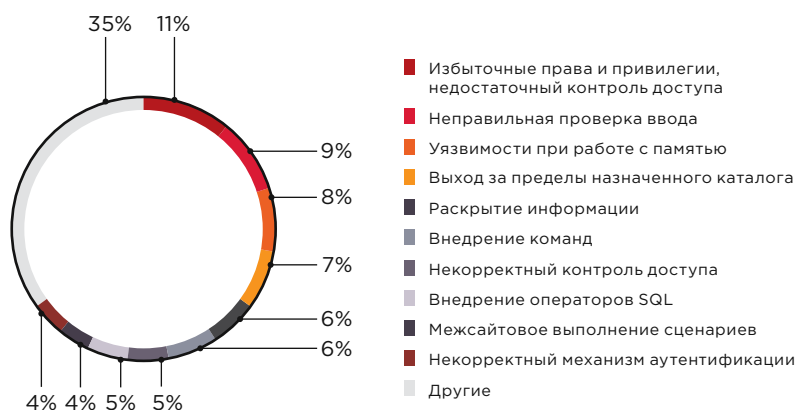


Рисунок 4. Типы уязвимостей компонентов АСУ ТП

Распределение уязвимостей по их воздействию

Около 75% уязвимостей связаны с возможным нарушением доступности (полным или частичным) компонентов АСУ ТП. Эксплуатация таких уязвимостей, к примеру, в сетевом оборудовании может нарушить сетевое взаимодействие и негативно повлиять на технологический процесс; сетевое оборудование — один из ключевых элементов АСУ ТП, поскольку оно обеспечивает передачу команд между компонентами.

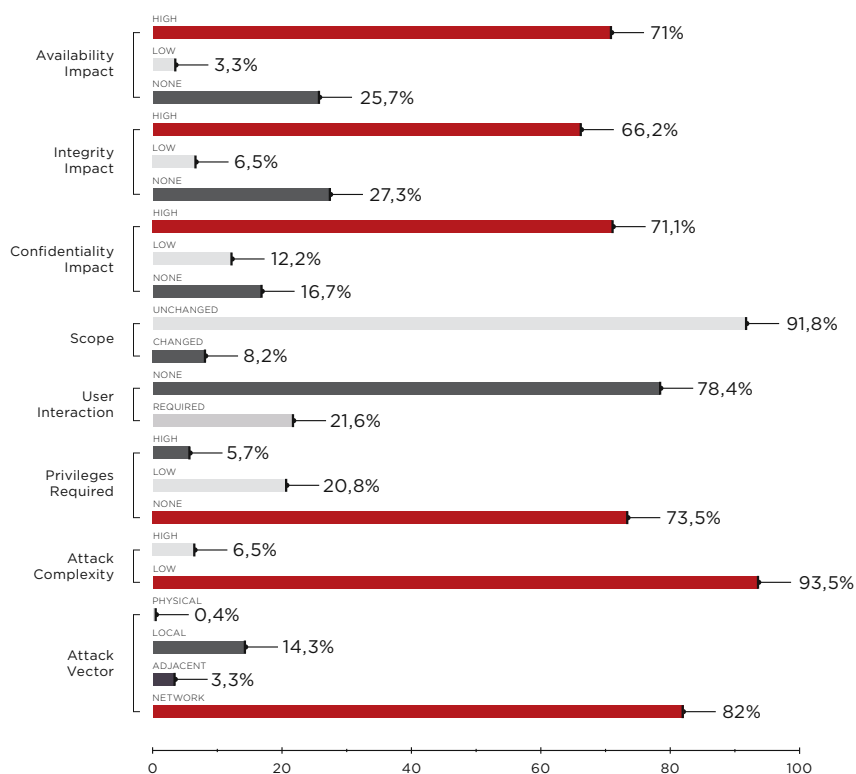


Рисунок 5. Значения метрик CVSS (указаны доли уязвимостей)

Распределение уязвимостей по степени риска

Больше половины выявленных уязвимостей относятся к критической и высокой степеням риска в соответствии с оценкой CVSS версии 3. При этом доля таких уязвимостей выросла на 17% по сравнению с предыдущим годом.

Если уязвимость имеет высокую степень риска, то в большинстве случаев она ставит под удар сразу три свойства безопасности информации — конфиденциальность, целостность и доступность. В 2018 году такое комплексное воздействие имели 58% уязвимостей. При этом среди них только для 4% сложность атаки была оценена как высокая. Это означает, что в большинстве случаев злоумышленнику не требуется никаких специальных условий, чтобы нарушить защищенность элементов АСУ ТП.



Рисунок 6. Степень риска уязвимостей

Краткие сведения об уязвимостях в компонентах АСУ ТП, выявленных специалистами Positive Technologies

За 2018 и начало 2019 года была опубликована информация о 54 уязвимостях, обнаруженных нашими экспертами в компонентах АСУ ТП таких производителей, как ABB, B&R Automation, Hirshmann, Moxa, Phoenix Contact, Schneider Electric и Siemens. При этом 14 из них присвоена критическая, а 11 — высокая степень риска.

Например, в коммутаторах Мокса была обнаружена возможность подбора учетных данных с использованием проприетарного протокола на порте 4000/TCP, которая позволяет получить контроль как над коммутатором, так и, возможно, над всей промышленной сетью. Отметим, что для получения актуальной версии прошивки с исправлением данной уязвимости конечный пользователь должен самостоятельно запросить ее у производителя.

Информация о других уязвимостях, найденных нашими экспертами, доступна на сайте [Positive Technologies](https://positive-technologies.com).

Распространенность компонентов АСУ ТП в интернете

Методика исследования

Исследование содержит результаты сканирования портов ресурсов, доступных в интернете. Для сканирования использовались общедоступные поисковые системы — Shodan (shodan.io), Google, Censys (censys.io). Сервис Shodan сканирует ограниченное число портов и производит сканирование 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.

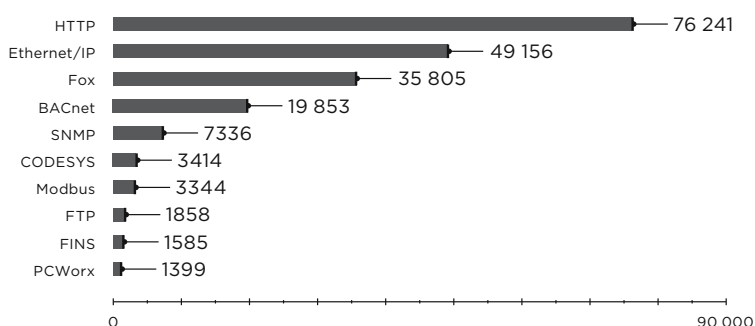


Рисунок 7. Количество компонентов АСУ ТП, доступных в интернете (топ-10 протоколов)

Распространенность

В результате исследования было выявлено 224 017 компонентов АСУ ТП, доступных в интернете. Это на 27% больше, чем в 2017 году.

Как и ранее, самым распространенным протоколом является HTTP. В 2018 году устройств АСУ ТП, поддерживающих протокол HTTP, примерно на 10 тысяч больше, чем в предыдущем.

При этом количество устройств, поддерживающих протокол Ethernet/IP, увеличилось на 25% по сравнению с 2017 годом, в результате чего он стал вторым по распространенности после HTTP. Количество же устройств, доступных по протоколу Fox, уменьшилось на 9%.

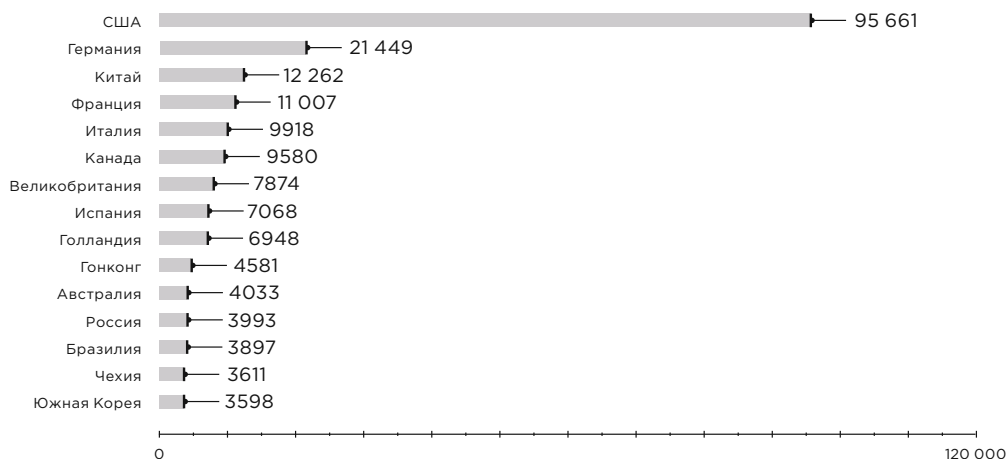


Рисунок 8. Количество компонентов АСУ ТП, доступных в интернете (топ-15 стран)

Территориальное распределение

Распределение по странам по сравнению с 2017 годом практически не изменилось. На первом месте по количеству найденных в интернете компонентов АСУ ТП остаются США, при этом их доля выросла на треть и составляет 42% от общего числа. Стоит отметить, что в топ-15 вошла Россия, которая в 2017 году была только на 28-м месте, а теперь занимает 12-е (3993 устройства).

Распределение по производителям и продуктам

Распределение по производителям за последний год практически не поменялось. На момент исследования было доступно около 30 тысяч устройств компании Honeywell, это ненамного больше, чем в прошлом году (разница около 7%), но стоит отметить, что такая динамика сохраняется из года в год.

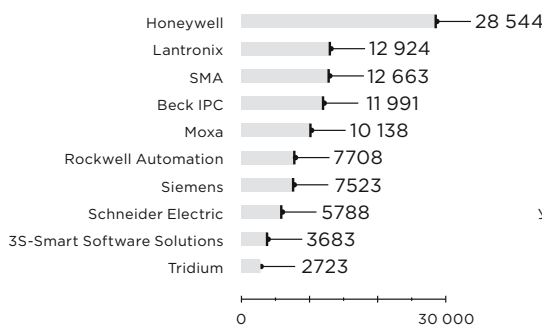


Рисунок 9. Количество компонентов АСУ ТП, доступных в интернете (топ-10 производителей)

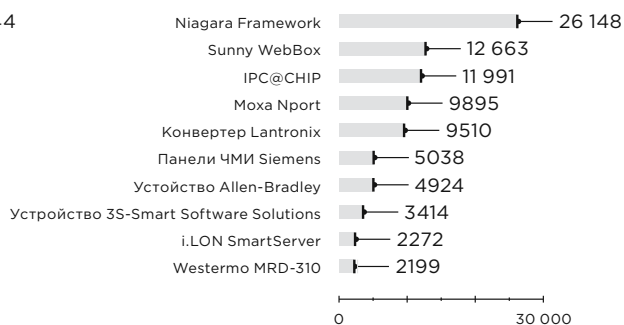


Рисунок 10. Количество компонентов АСУ ТП, доступных в интернете (топ-10 продуктов)

Доля продукта Niagara Framework, соответственно, тоже немного увеличилась (примерно на 5%).

Типы компонентов АСУ ТП

Почти треть компонентов, доступных в интернете (27%), относится к системам управления (SCADA, ЧМИ, РСУ). На 6% увеличились доли сетевых устройств и ПЛК (в прошлом году было по 13%).

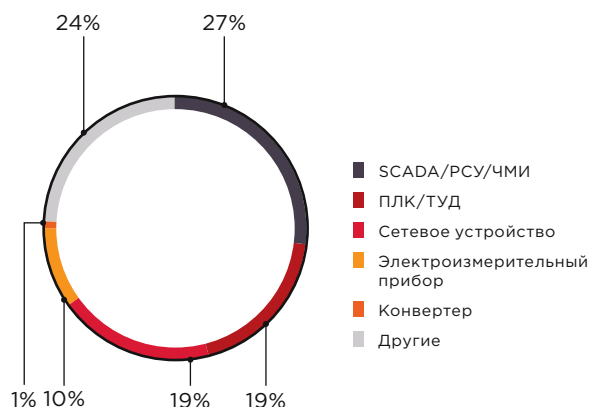


Рисунок 11. Количество компонентов АСУ ТП, доступных в интернете (распределение по типу)

Заключение

Как показывает наша статистика, количество уязвимостей, выявляемых в оборудовании различных производителей, из года в год растет, а количество доступных в интернете компонентов АСУ ТП не снижается. Количество уязвимостей основных производителей в 2018 году увеличилось на 30% по сравнению с 2017 годом, при этом доля уязвимостей высокой и критической степени риска выросла на 17%.

При этом нужно отметить, что среднее время устранения уязвимостей вендором остается достаточно долгим (более 6 месяцев). Иногда исправление отдельных уязвимостей (от уведомления производителя до выпуска обновлений) занимает более двух лет. Для конечного пользователя тот факт, что обновления не выпускаются оперативно, повышает риски возможной эксплуатации уязвимостей в принадлежащем ему оборудовании.

Количество компонентов сети АСУ ТП, доступных в интернете, с прошлого года выросло на 27% и теперь составляет более 220 тысяч. Большая часть из них относится к различным системам автоматизации. Наибольшее количество таких систем находится в США, Германии, Китае, Франции, Италии и Канаде — даже несмотря на то, что вопрос безопасности подобных устройств и систем уже давно интересует местных законодателей. Например, для оборудования, которое используется на различных промышленных предприятиях, Международная организация по стандартизации недавно выпустила новое руководство, целью которого является снижение риска кибератак.

Наше исследование в очередной раз доказывает, что в настоящее время компоненты АСУ ТП нельзя назвать полностью защищенными. Вопросам их безопасности необходимо уделять пристальное внимание, а при отсутствии адекватной защиты таких компонентов всегда существует риск нарушения штатного режима их работы.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. 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.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.