БЕЗОПАСНОСТЬ АСУ ТП: ИТОГИ 2016 ГОДА

POSITIVE TECHNOLOGIES

ВВЕДЕНИЕ

Применение автоматизированных систем управления технологическим процессом, или промышленных систем управления (АСУ ТП, ICS) уже давно вышло за рамки классических промышленных организаций. Сегодня компоненты АСУ ТП применяются в самых разных областях, от атомных электростанций до персональных систем «умных домов». Быстрый рост числа компаний, внедряющих АСУ ТП, при ограниченном числе ведущих производителей приводит к тому, что один и тот же продукт может использоваться как на критически важных объектах, так и в частных организациях. Злоумышленник, обнаружив уязвимость в одном компоненте АСУ ТП, сможет проводить атаки на множество объектов во всем мире. Между тем производители и потребители не всегда уделяют должное внимание безопасности своих АСУ ТП. Из-за требования непрерывности технологических процессов базовые компоненты систем управления (индустриальные протоколы, ОС, СУБД) не обновляются годами. Все эти факторы в совокупности приводят к развитию новых угроз безопасности.

В частности, как выявило наше исследование, в 2016 году было опубликовано более 100 уязвимостей в компонентах АСУ ТП основных производителей, больше всего их найдено в продуктах Siemens, Advantech, Schneider Electric и Moxa. Основная доля опубликованных уязвимостей имеет критическую и высокую степень риска (60%), наиболее распространенные из них это «Удаленное выполнение кода», «Отказ в обслуживании» и «Раскрытие информации». При этом большая часть уязвимостей приходится на устройства диспетчеризации и мониторинга (ЧМИ/SCADA).

Кроме того, на начало 2017 года обнаружено более 160 000 компонентов АСУ ТП, имеющих подключение к сети Интернет. Наибольшее их количество приходится на США (31%), Германию (8%) и Китай (5%). Как и в прошлые годы, самыми распространенными компонентами в сети Интернет являются системы автоматизации зданий компании Tridium, системы мониторинга и управления электроэнергией SMA Solar Technology, а также устройство IPC@CHIP немецкой компании Beck IPC.

Более подробные результаты анализа уязвимостей и доступных через сеть Интернет компонентов АСУ ТП приведены ниже.

СПИСОК ОСНОВНЫХ СОКРАЩЕНИЙ

OPC — object linking and embedding for process control / семейство программных технологий, предоставляющих единый интерфейс для управления объектами автоматизации и технологическими процессами

RTU (ТУД) — remote terminal unit / терминал удаленного доступа и управления

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

РСУ — распределенные системы управления

ЧМИ — человеко-машинный интерфейс

АНАЛИЗ УЯЗВИМОСТЕЙ КОМПОНЕНТОВ АСУ ТП

Методика исследования

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 блогах[1].

В качестве базы знаний уязвимостей использовались следующие ресурсы:

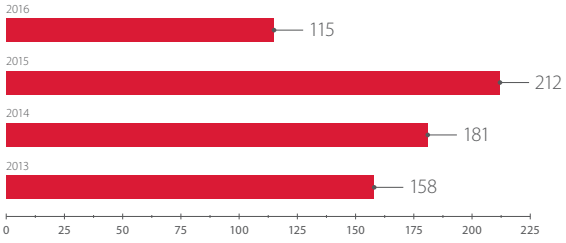
+ ICS-CERT (ics-cert.us-cert.gov)
+ NVD (nvd.nist.gov), CVE (cve.mitre.org)
+ Positive Research Center (securitylab.ru/lab)
+ Siemens Product CERT (siemens.com/cert)
+ Schneider Electric Cybersecurity Support Portal (schneider-electric.com/b2b/en/support/cybersecurity/security-notifications.jsp)

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

При анализе уязвимостей было рассмотрено оборудование и ПО ведущих производителей автоматизированных систем. При этом в исследование не включались данные по уязвимостям общераспространенного ПО (например, OpenSSL или GNU), которое могло быть использовано при разработке прикладного ПО для АСУ ТП.

Динамика обнаружения уязвимостей

По сравнению с 2015 годом в 2016 году количество опубликованных уязвимостей основных производителей снизилось (115). Следует отметить, что такое количество уязвимостей нельзя назвать окончательным, так как данные по некоторым из них могут быть опубликованы позднее, после их устранения. В частности, эксперты нашей компании направили производителям систем АСУ ТП (Siemens, Schneider Electric и др.) информацию о 13 уязвимостях, которые на момент написания данной статьи еще не опубликованы.

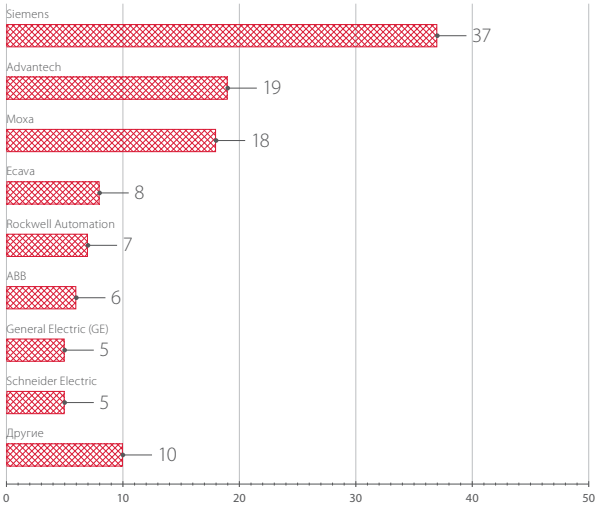


Общее количество уязвимостей, обнаруженных в компонентах АСУ ТП

Уязвимости по производителям

Как и в 2015 году, лидерами в рейтинге наиболее уязвимых компонентов АСУ ТП являются продукты компаний Siemens, Advantech, Schneider Electric, а также производителя промышленного сетевого оборудования компании Moxa. Количество опубликованных уязвимостей напрямую зависит от распространенности продукта и от того, придерживается ли производитель политики ответственного разглашения. Поэтому эти данные не свидетельствуют напрямую о недостаточной защищенности этих решений. Скорее может быть справедливым обратный вывод: продукты производителей, не публикующих информацию о выявленных и исправленных уязвимостях, вероятно, более уязвимы.

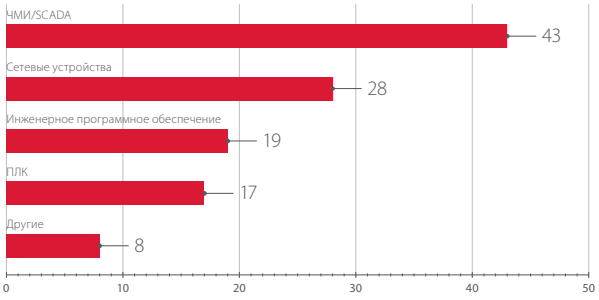
1 digitalbond.com, scadahacker.com, immunityinc.com/products/canvas, exploit-db.com, rapid7.com/db



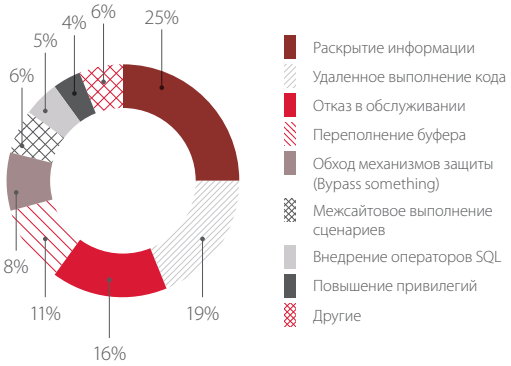
Уязвимости по основным производителям компонентов АСУ ТП

Уязвимости по компонентам

Большая часть уязвимостей, опубликованных в 2016 году, приходится на устройства, выполняющие функции диспетчеризации и мониторинга (ЧМИ/SCADA). А наиболее распространенными типами уязвимостей стали «Удаленное выполнение кода», «Отказ в обслуживании» и «Раскрытие информации».

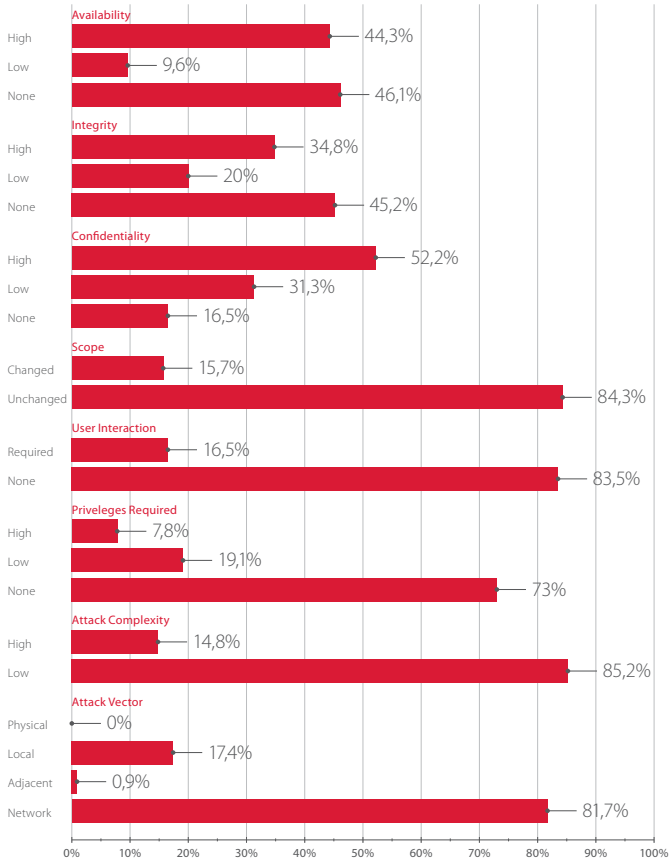


Количество уязвимостей в различных компонентах АСУ ТП



Распространенные типы уязвимостей компонентов АСУ ТП

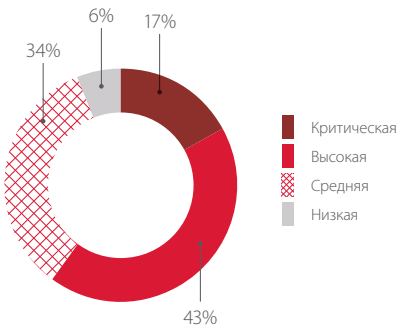
При этом, в соответствии с метриками CVSS версии 3, большинство уязвимостей могут эксплуатироваться удаленно без необходимости получения каких-либо привилегий.



Доля уязвимостей в соответствии со значениями метрик CVSS

Степень риска

Больше половины выявленных уязвимостей относятся к критической и высокой степени риска в соответствии с оценкой CVSS версии 3.



Распределение уязимостей по степеням риска

Уязвимости, выявленные специалистами Positive Technologies

В 2016 году производители подтвердили и устранили 11 новых уязвимостей, выявленных нашими специалистами в компонентах АСУ ТП таких компаний, как Siemens, Advantech, Schneider Electric, General Electric, Rockwell Automation. Две обнаруженные уязвимости имеют критическую степень риска, еще две — высокую.

Таблица 1. Примеры обнаруженных уязвимостей

	ICSA-16-336-01 (CVE-2016-8567)	SEVD-2016-343-01	ICSA-16-336-05A (CVE-2016-9360)
Производитель	**Siemens**	**Schneider Electric**	**General Electric**
Краткое описание	Уязвимость в программном обеспечении Siemens SICAM Power Automation System связана с ненадежным хранением паролей и разглашением чувствительной информации. Злоумышленник может удаленно получить привилегированный доступ к базе данных SICAM PAS, используя стандартную возможность дистанционного конфигурирования через TCP-порт 2638 и жестко закодированные пароли в заводских учетных записях	Уязвимость в программном обеспечении StruxureWare Data Center Expert 7.3.1.114 и 7.2.4 и более ранних версиях продукта связана с небезопасным хранением некоторых паролей в открытом виде в оперативной памяти	Уязвимость в продуктах Proficy HMI/SCADA iFIX 5.8 SIM 13, Proficy HMI/SCADA CIMPLICITY 9.0, Proficy Historian 6.0 и в их предыдущих версиях позволяет злоумышленнику локально перехватить пароли пользователей при наличии доступа к авторизованной сессии
Оценка CVSS	**9,8** Уязвимость критического уровня риска	**7,6** Уязвимость высокого уровня риска	**6,4** Уязвимость среднего уровня риска
Вектор CVSS	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N	AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:L/A:L
Рекомендации по устранению	Для устранения уязвимости производитель рекомендует обновить SICAM PAS до версии 8.0	Для устранения уязвимости производитель рекомендует обновить программное обеспечение до версии 7.4.0 или выше	Для устранения уязвимости производитель рекомендует обновить Proficy HMI/SCADA iFIX до версии 5.8 SIM 14, Proficy HMI/SCADA CIMPLICITY — до версии 9.5, а Proficy Historian — до версии 7.0
Ссылка	ics-cert.us-cert.gov/advisories/ICSA-16-336-01	schneider-electric.com/en/download/document/SEVD-2016-343-01	ics-cert.us-cert.gov/advisories/ICSA-16-336-05A

РАСПРОСТРАНЕННОСТЬ КОМПОНЕНТОВ АСУ ТП В СЕТИ ИНТЕРНЕТ

Методика исследования

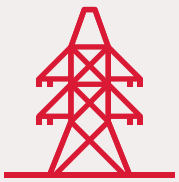
Сбор данных о доступности компонентов АСУ ТП в сети Интернет осуществлялся исключительно пассивными методами. Использовались результаты сканирования портов ресурсов, доступных в сети Интернет, полученные с помощью общедоступных поисковых систем: Google, Shodan (shodan.io), Censys (censys.io).

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, состоящую примерно из 800 записей, позволяющих на основе баннера сделать заключение об используемом продукте и его производителе.

Распространенность

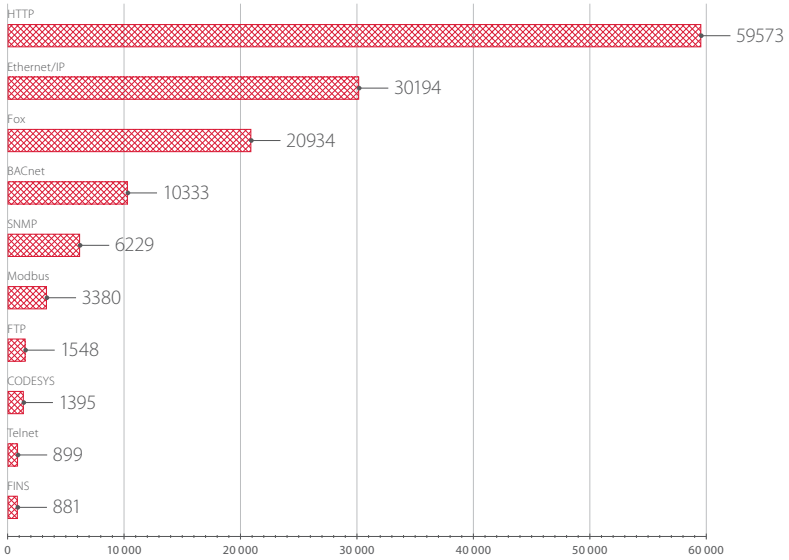
В результате исследования выявлено 162 039 компонентов АСУ ТП, доступных в сети Интернет. Установлено, что 4515 компонентов (3% от общего числа) применяются в области энергетики, а 38 580 (24%) относятся к области автоматизации зданий.

Если рассматривать доступные компоненты в зависимости от используемого ими протокола, то было выявлено, что наибольшее количество компонентов АСУ ТП, как и в прошлые годы, доступно по протоколу HTTP.



Важно

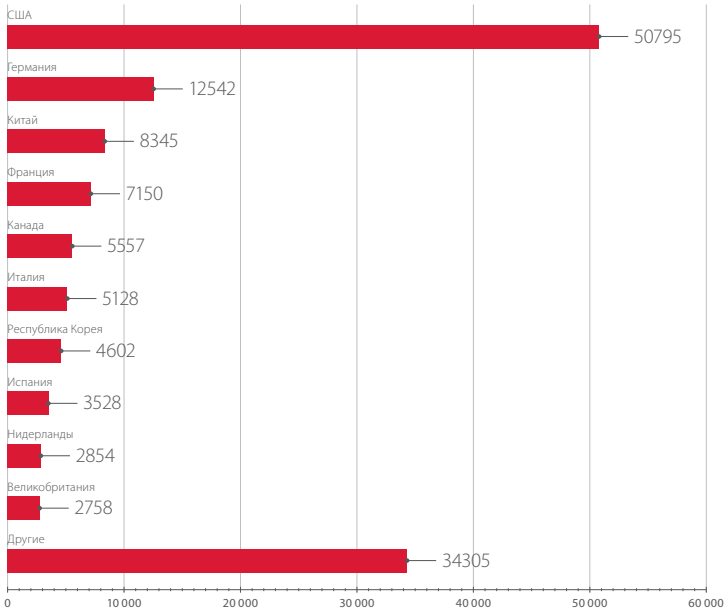
Уязвимости, связанные с хранением паролей пользователей в открытом виде, могут привести к перехвату контроля над SCADA-системой. Штатно авторизовавшись в системе, злоумышленник может влиять на технологический процесс, что грозит не только экономическими потерями, но и поломкой оборудования и даже авариями. А в случае получения пароля к базам данных злоумышленник может нелегитимно модифицировать информацию, создавая предпосылки к возникновению различных нештатных ситуаций.



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

Территориальное распределение

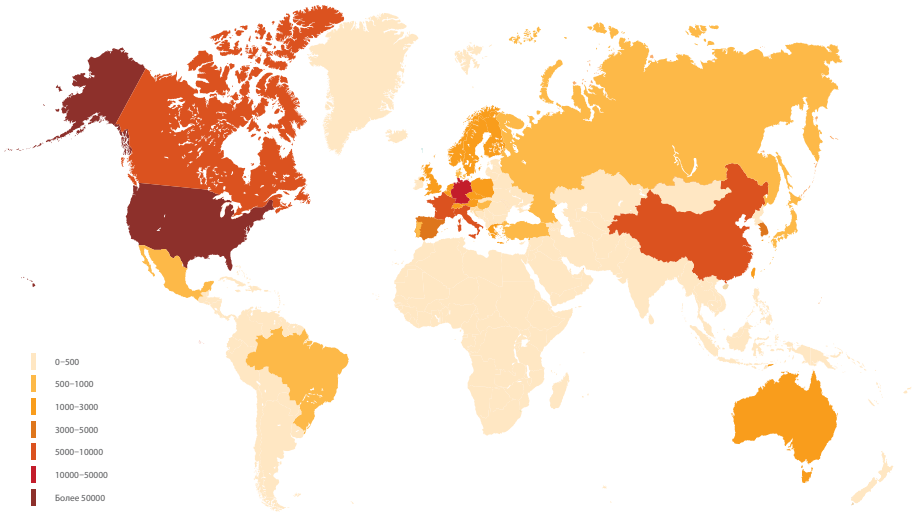
Лидером по количеству найденных компонентов с большим отрывом уже не первый год является США (31% от общего числа найденных компонентов), второе место занимает Германия (8%), затем следует Китай (5%), который в 2015 году даже не попал в первую десятку лидеров. Большое число найденных компонентов АСУ ТП в этих странах, среди прочего, связано с широким распространением современных автоматизированных систем управления зданиями.



Топ-10 стран по количеству компонентов АСУ ТП, доступных в сети Интернет

Интересный факт

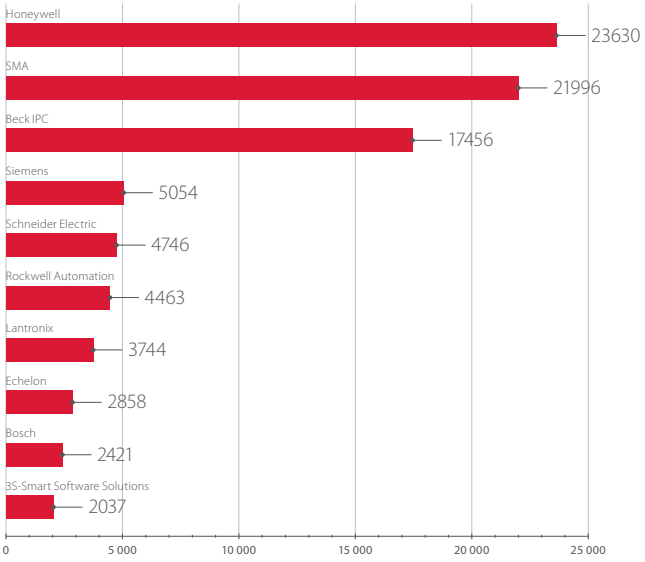
Как и в прошлый период, в 2016 году Россия занимает 31 место с 591 компонентом АСУ ТП (менее 1% от общего числа доступных в сети Интернет компонентов).



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

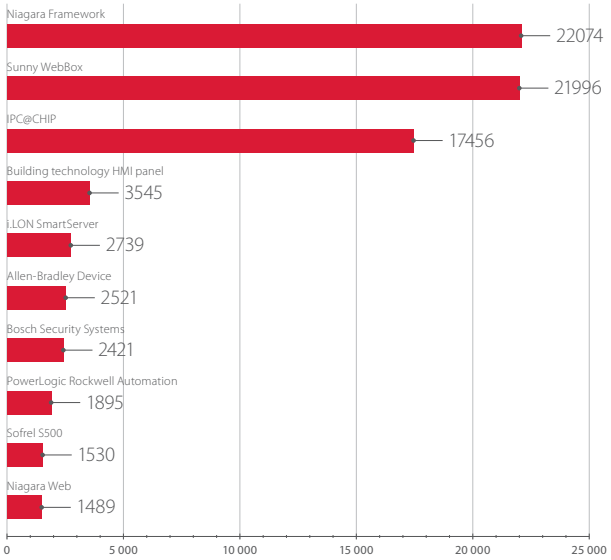
Распространенность компонентов АСУ ТП по производителям

Программный продукт Niagara Framework компании Honeywell по-прежнему лидирует по количеству доступного в сети Интернет оборудования. С минимальным отрывом на втором месте находится компания SMA Solar Technology со своим продуктом Sunny WebBox. Третье место заняла немецкая компания Beck IPC с устройством IPC@CHIP.



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

Система Niagara Framework компании Tridium, входящей в состав корпорации Honeywell, — одна из самых распространенных систем для автоматизации технологических процессов в «умных домах». Система мониторинга и управления электроэнергией на основе технологий солнечных батарей Sunny WebBox компании SMA Solar Technology особенно популярна в европейских странах. Распространенность микросхем IPC@CHIP фирмы Beck IPC объясняется их относительно низкой ценой, многофункциональностью и наличием встроенного контроллера Ethernet с поддержкой стека TCP/IP и встроенного веб-сервера.



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

Типы доступных компонентов АСУ ТП

При составлении базы данных идентификаторов была добавлена информация о типе того или иного компонента АСУ ТП.

Таблица 2. Соотношение различных компонентов АСУ ТП, доступных в сети Интернет

Тип компонента АСУ ТП	Доля в 2016 году	Доля в 2015 году
SCADA/РСУ/ЧМИ+ПЛК/ТУД (RTU)	13,62% ↓	15,98%
ТУД/ПЛК	12,86% ↑	11,53%
SCADA/РСУ/ЧМИ	7,80% ↓	8,53%
Электроизмерительный прибор	5,18% ↓	11,37%
Сетевое устройство	5,06% ↑	3,17%
Конвертер интерфейсов	1,31% ↑	0,26%
Автоматический выключатель	0,15% ↓	0,23%
Инвертор	0,15% ↑	0,01%
Сенсор	0,13% ↓	0,57%
Релейная защита и автоматика	0,01%	0,01%
Другие компоненты	53,72% ↑	48,33%

Интересный факт

Конвертеры интерфейсов и сетевые устройства представляют наибольший интерес для злоумышленников. Атаки на подобные устройства не требуют понимания технологического процесса и могут привести к его нарушениям и даже к серьезным авариям.

ЗАКЛЮЧЕНИЕ

По итогам 2016 года отмечается значительное снижение количества уязвимостей, опубликованных основными производителями компонентов АСУ ТП, так как большая часть уязвимостей в распространенных продуктах была устранена в предыдущие годы. При этом больше половины выявленных уязвимостей имеют критическую и высокую степень риска, поскольку именно такие уязвимости стараются устранить в первую очередь. Важно отметить, что ведущие производители стали уделять больше внимания выявлению и устранению уязвимостей как на этапе разработки своих продуктов, так и в процессе эксплуатации. Активное сотрудничество производителей с исследователями в области информационной безопасности позволяет значительно повысить общий уровень защищенности компонентов АСУ ТП.

С другой стороны, количество компонентов АСУ ТП, доступных в сети Интернет, увеличивается с каждым годом. Наибольшее их количество обнаружено в странах, в которых системы автоматизации развиты лучше всего (США, Германия, Китай, Франция, Канада). Большинство компонентов АСУ ТП, доступных в сети Интернет, многофункциональны и применяются для автоматизации технологических процессов в самых разных системах. Для удаленного доступа к компонентам АСУ ТП часто используются словарные или сервисные пароли, что позволяет любому злоумышленнику без труда перехватить управление над системой. При этом минимальные превентивные меры защиты, такие как отключение компонентов АСУ ТП от сети Интернет и использование сложных паролей, позволяют в значительной степени снизить вероятность проведения атак.

Для повышения общего уровня безопасности необходимо проводить регулярный анализ защищенности АСУ ТП с целью выявления возможных векторов атак и разработки эффективной системы защиты. Кроме того, о выявлении новых уязвимостей и недекларированных возможностей в компонентах АСУ ТП в процессе их эксплуатации необходимо своевременно сообщать производителям.

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.

POSITIVE TECHNOLOGIES

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