

# БЕЗОПАСНОСТЬ АСУ ТП В ЦИФРАХ

Евгений Дружинин, Илья Карпов, Евгений Гнедин,  
Иван Бойко, Юлия Симонова



## 2016

POSITIVE TECHNOLOGIES

## Оглавление

Введение.....	3
Список сокращений.....	4
1. Результаты.....	5
2. Методика исследования.....	5
2.1. Методика исследования уязвимостей компонентов АСУ ТП.....	5
2.2. Методика исследования распространенности компонентов АСУ ТП в сети Интернет.....	7
3. Анализ уязвимостей компонентов АСУ ТП.....	7
3.1. Динамика обнаружения уязвимостей.....	7
3.2. Количество уязвимостей в компонентах АСУ ТП различных производителей.....	8
3.3. Уязвимости различных компонентов АСУ ТП.....	9
3.4. Степень риска выявленных уязвимостей.....	9
3.5. Доля устраненных уязвимостей в компонентах АСУ ТП и возможности для проведения атак.....	11
3.6. Распределение уязвимостей по типу.....	12
4. Распространенность компонентов АСУ ТП в сети Интернет.....	13
4.1. Распространенность компонентов АСУ ТП.....	13
4.2. Территориальное распределение компонентов АСУ ТП.....	13
4.3. Распространенность компонентов АСУ ТП по производителям и продуктам.....	15
4.4. Типы компонентов АСУ ТП.....	17
4.5. Количество уязвимых компонентов АСУ ТП.....	18
Заключение.....	19

## Введение

Современный мир уже невозможно представить без средств автоматизации. Редко можно увидеть крупный завод, производство на котором построено исключительно на аналоговых регуляторах и релейных схемах. Использование автоматизированных систем управления технологическими процессами выгодно предприятию как с экономической, так и с практической точки зрения. Термин АСУ ТП появился в 80-е годы, и основными объектами автоматизации являлись тогда крупные предприятия. Однако в результате развития и удешевления техники, а также постоянного развития информационных технологий, за прошедшие десятилетия АСУ ТП получили более широкое применение и вышли за рамки одного только крупного производства. Современные АСУ ТП применяются в различных областях — от управления домашним освещением до атомных электростанций.

Многие компьютеризированные системы «умных домов» построены на технологиях, аналогичных тем, что используются на промышленных предприятиях, а модернизированные системы контроля электроснабжения (smart grid) расширяют промышленную сеть до жилых домов и отдельных квартир. В 2014 году специалисты Positive Technologies опубликовали исследование о безопасности таких систем, показавшее их недостаточную защищенность<sup>1</sup>.

Развитие АСУ ТП в современном, цифровом, исполнении, а также частое применение широко распространенных технологий позволяет потенциальному нарушителю эксплуатировать уязвимости, характерные не только для АСУ ТП, но и другие, свойственные любым сетевым инфраструктурам на основе технологии Ethernet.

Современная тенденция к интегрированию АСУ ТП в сети предприятий с доступом к глобальной сети, их доступность и возможность их удаленной эксплуатации привели к возникновению и развитию различного вредоносного ПО (Stuxnet, Duqu, Flame, Havex, BlackEnergy), а также к появлению принципиально новых угроз. Постоянно публикуются новые уязвимости, найденные в различном промышленном оборудовании. К примеру, недавно опубликовано исследование об уязвимостях высокой степени риска, обнаруженных в медицинском оборудовании CareFusion<sup>2</sup>. Однако защита АСУ ТП — непростой вопрос, в первую очередь из-за сложной организации таких систем и требований непрерывности технологического процесса.

Следует отметить, что вопросам обеспечения безопасности АСУ ТП стали уделять пристальное внимание и государственные органы. После утверждения в 2012 году Президентом РФ документа «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» и публикации поручения Президента РФ от 15.11.2011 № Пр-3400 «Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года» появились новые документы, рассматривающие вопросы обеспечения безопасности информации в АСУ ТП.

В дополнение к имеющимся документам по ключевым системам информационной инфраструктуры был выпущен приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных

<sup>1</sup> [ptsecurity.ru/download/Smart\\_Grid\\_Vulnerabilities.pdf](http://ptsecurity.ru/download/Smart_Grid_Vulnerabilities.pdf)

<sup>2</sup> [ics-cert.us-cert.gov/advisories/ICSMA-16-089-01](http://ics-cert.us-cert.gov/advisories/ICSMA-16-089-01)

объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Эксперты Positive Technologies сопоставили новые требования с ведущими зарубежными стандартами в области промышленной автоматизации (NERC CIP, ISA/IEC 62443, NIST SP 800-82 и 800-53)<sup>3</sup>. Также на сайте ФСТЭК появилась база угроз и база уязвимостей, включающая, как и зарубежные аналоги, уязвимости и угрозы, связанные с АСУ ТП (bdu.fstec.ru).

Стоит отметить и интерес к своевременному выявлению и устранению уязвимостей со стороны производителей (применение политики ответственного разглашения, взаимодействие с исследователями). Этим, в частности, можно объяснить практически неизменное количество выявленных уязвимостей в период с 2012 по 2015 год (в отличие от исследований, проведенных ранее). В 2012 году компания Positive Technologies выпустила аналитический отчет «Безопасность промышленных систем в цифрах», где была продемонстрирована доступность большого количества компонентов АСУ ТП через сеть Интернет<sup>4</sup>. Согласно этому исследованию, за три года (2010–2012) число уязвимостей в АСУ ТП выросло в 20 раз (с 9 до 192).

Настоящий отчет обобщает имеющиеся сведения, полученные за период с 2012 по 2015 год и дает возможность оценить произошедшие изменения. Он состоит из двух частей и представляет результаты анализа уязвимостей компонентов АСУ ТП и их распространенности в сети Интернет.

## Список сокращений

**OPC** — object linking and embedding for process control.

**RTU** — remote terminal unit.

**SCADA** — supervisory control and data acquisition.

**АРМ** — автоматизированное рабочее место.

**АСУ ТП** — автоматизированная система управления технологическим процессом.

**АСУЗ** — автоматизированные системы управления зданиями.

**ПЛК** — программируемый логический контроллер.

**РЗА** — релейная защита и автоматика.

**PCU** — распределенные системы управления.

**ТУД** — терминал удаленного доступа и управления.

**ЧМИ** — человеко-машинный интерфейс.

<sup>3</sup> [ptsecurity.ru/download/FSTEC\\_N31\\_NERK\\_NIST\\_ISA\\_IEC.pdf](http://ptsecurity.ru/download/FSTEC_N31_NERK_NIST_ISA_IEC.pdf)

<sup>4</sup> [ptsecurity.ru/download/SCADA\\_analytics\\_russian.pdf](http://ptsecurity.ru/download/SCADA_analytics_russian.pdf)

## 1. Результаты

В рамках исследования были рассмотрены компоненты АСУ ТП различных производителей. В период с 2012 по 2015 год всего было выявлено 743 уязвимости в компонентах АСУ ТП; наибольшее количество — у наиболее известных компаний: Siemens, Schneider Electric и Advantech. При этом основная доля уязвимостей имеет высокую и среднюю (по 47%) степень риска. Если оценивать уровень опасности уязвимости исходя из возможности реализации главных угроз информационной безопасности (нарушения конфиденциальности, целостности и доступности) в результате ее эксплуатации, то больше половины выявленных уязвимостей имеют высокую метрику по такому важному показателю, как нарушение доступности, играющему ключевую роль в АСУ ТП. В совокупности с возможностью удаленной эксплуатации уязвимостей и слабыми механизмами аутентификации это значительно повышает риск проведения атак.

С помощью общедоступных поисковых систем по состоянию на март 2016 года обнаруживаются более 150 000 различных компонентов АСУ ТП, имеющих подключение к сети Интернет. Причем в большинстве случаев для авторизации в такой системе используется словарный пароль. Наибольшее число компонентов АСУ ТП было найдено в США (43%), Германии (12%), Франции, Италии и Канаде (примерно по 5%).

Самыми распространенными компонентами в сети Интернет являются системы для автоматизации зданий компании Tridium (25 264), входящей в состав группы компаний Honeywell, а также системы мониторинга и управления электроэнергией, в том числе на основе технологий солнечных батарей компании SMA Solar Technology (17 275).

В ходе исследования были найдены автоматизированные системы, управляющие производственными процессами различных предприятий, транспортом, водоснабжением и энергоресурсами. При отсутствии адекватной защиты таких систем злоумышленнику не обязательно обладать какими-то специальными знаниями, чтобы получить к ним доступ, а его действия могут привести к серьезным последствиям.

## 2. Методика исследования

### 2.1. Методика исследования уязвимостей компонентов АСУ ТП

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<sup>5</sup>.

В качестве базы знаний уязвимостей использовались следующие ресурсы:

- + ICS-CERT ([ics-cert.us-cert.gov](http://ics-cert.us-cert.gov)),
- + NVD ([nvd.nist.gov](http://nvd.nist.gov)), CVE ([cve.mitre.org](http://cve.mitre.org)),
- + Positive Research Center ([securitylab.ru/lab/](http://securitylab.ru/lab/)),
- + Siemens Product CERT ([siemens.com/cert](http://siemens.com/cert)).

В базах знаний уязвимостей нет указания на специализацию тех или иных продуктов. Для определения принадлежности уязвимого продукта к АСУ ТП был сформирован список компаний, предоставляющих решения в сфере автоматизации. При подготовке списка мы использовали знания и опыт наших специалистов, полученные в ходе консалтинговых

<sup>5</sup> [digitalbond.com](http://digitalbond.com), [scadahacker.com](http://scadahacker.com), [immunityinc.com/products/canvas](http://immunityinc.com/products/canvas), [exploit-db.com](http://exploit-db.com), [rapid7.com/db/](http://rapid7.com/db/)

работ, а также перечень продуктов и компаний, опубликованный на ICS-CERT, и ряд специализированных аналитических ресурсов (arcweb.com, controlglobal.com, technavio.com).

Учитывались отношения между компаниями-производителями. Например, компания Schneider Electric приобрела компанию Invensys в 2014 году, и в рамках исследования все выявленные уязвимости в компонентах Invensys были отнесены к уязвимостям компании Schneider Electric.

При исследовании учитывались особенности доступной информации об уязвимостях:

1. Одна из проблем типового описания уязвимостей — отсутствие строгой типизации описания производителя, продукта и версий. Возьмем, к примеру, CVE-2013-6030 и CVE-2014-2350: описания составлены в свободной форме.

---

#### CVE-2013-6030

*Directory traversal vulnerability on the Emerson Network Power Avocent MergePoint Unity 2016 (aka MPU2016) KVM switch with firmware 1.9.16473 allows remote attackers to read arbitrary files via unspecified vectors, as demonstrated by reading the /etc/passwd file.*

---

#### CVE-2014-2350

*Emerson DeltaV 10.3.1, 11.3, 11.3.1, and 12.3 uses hardcoded credentials for diagnostic services, which allows remote attackers to bypass intended access restrictions via a TCP session, as demonstrated by a session that uses the telnet program.*

2. Количество уязвимостей, публикуемых в списке CVE (Common Vulnerabilities and Exposures) регуляторами, различными CERT (computer emergency response teams) и производителями, не всегда отражает истинную ситуацию. Зачастую публикуются неполные данные из оригинального сообщения об уязвимостях (advisory), при этом производятся исправления не опубликованных уязвимостей.

Примером может служить новость ICS-CERT об устранении компанией Honeywell уязвимостей: в ней присутствуют описания и ссылки на 5 различных CVE, тогда как база данных OSVDB (osvdb.org) содержит оригинальный перечень из 24 уязвимостей<sup>6</sup>.

В худшем случае производитель не считает, что выявленная ошибка действительно является уязвимостью. Бывают даже случаи, когда производители отказываются принимать рекомендации не использовать стандартные запрограммированные (hardcoded) пароли, которые не могут быть изменены пользователем, не использовать удаленное выполнение команды (OS commanding) и отказываются признавать другие явные ошибки, позволяющие скомпрометировать систему и поддающиеся классификации на основе WASC (webappsec.org), OWASP (owasp.org) или CWE (cwe.mitre.org).

Степень риска уязвимости компонентов АСУ ТП мы определяли на основе значения Common Vulnerability Scoring System второй версии (first.org/cvss). Качественная оценка степени риска строится на типовом подходе:

- + 0,0 < CVSS ≤ 3,9 — низкая степень риска;
- + 4,0 ≤ CVSS ≤ 6,9 — средняя степень;
- + 7,0 ≤ CVSS ≤ 10,0 — высокая степень.

---

<sup>6</sup> [ics-cert.us-cert.gov/advisories/ICSA-14-352-01](https://ics-cert.us-cert.gov/advisories/ICSA-14-352-01)

## 2.2. Методика исследования распространенности компонентов АСУ ТП в сети Интернет

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, icsmap.shodan.io), Censys (scans.io, 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. В подавляющем большинстве идентификаторов использовались протоколы SNMP и HTTP/HTTPS — в связи с тем, что во многих АСУ ТП по протоколам HTTP/HTTPS представляется удобный и простой доступ к HMI, а по протоколу SNMP осуществляется доступ к большинству сетевых устройств. Кроме того, в большом количестве присутствовали идентификаторы для анализа промышленных протоколов, таких как Modbus TCP, S7, DNP3 over TCP/IP, BACnet IP, FINS.

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

- + Сервис Shodan использует 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 в баннерах информации об используемых версиях программного обеспечения.

Итак, полученная информация не обладает той полнотой, которая может быть достижима при активном сканировании, однако имеющиеся результаты достоверны, качественны и хорошо показывают доступность компонентов АСУ ТП в сети Интернет.

## 3. Анализ уязвимостей компонентов АСУ ТП

### 3.1. Динамика обнаружения уязвимостей

В рамках исследования были рассмотрены уязвимости компонентов порядка 500 производителей автоматизированных систем. В итоге было выявлено 743 уязвимости в АСУ ТП. Эксперты Positive Technologies в 2015 году обнаружили 7 новых уязвимостей<sup>7</sup> (2 из них имеют высокую степень риска), подробная информация о которых была направлена производителю.

Количество обнаруживаемых каждый год уязвимостей в период с 2012<sup>8</sup> по 2015 год остается практически неизменным. Это можно объяснить возросшим интересом производителей оборудования к своевременному выявлению и устранению уязвимостей и взаимодействию с исследователями.

<sup>7</sup> [ptsecurity.ru/research/threatscape](http://ptsecurity.ru/research/threatscape), [securitylab.ru/lab](http://securitylab.ru/lab).

<sup>8</sup> Данные о количестве уязвимостей, представленные в отчете за 2012 год, отличаются от нынешних, поскольку некоторые уязвимости 2012 года были опубликованы позже.

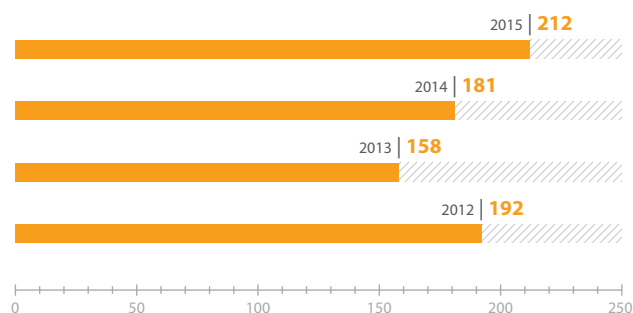


Рис. 1. Общее количество уязвимостей, обнаруженных в компонентах АСУ ТП

### 3.2. Количество уязвимостей в компонентах АСУ ТП различных производителей

Как и в 2012 году, лидерами в рейтинге наиболее уязвимых компонентов АСУ ТП являются продукты Siemens, Schneider Electric и Advantech. Количество уязвимостей в компонентах АСУ ТП различных производителей представлено на рис. 2. В категорию «Другие» вошел 81 производитель: их продукты имеют меньше 5 уязвимостей.

Количество обнаруженных уязвимостей зависит от распространенности продукта и от того, придерживается ли производитель политики ответственного разглашения. Как следствие, эти данные не свидетельствуют напрямую о защищенности конкретных решений того или иного производителя.

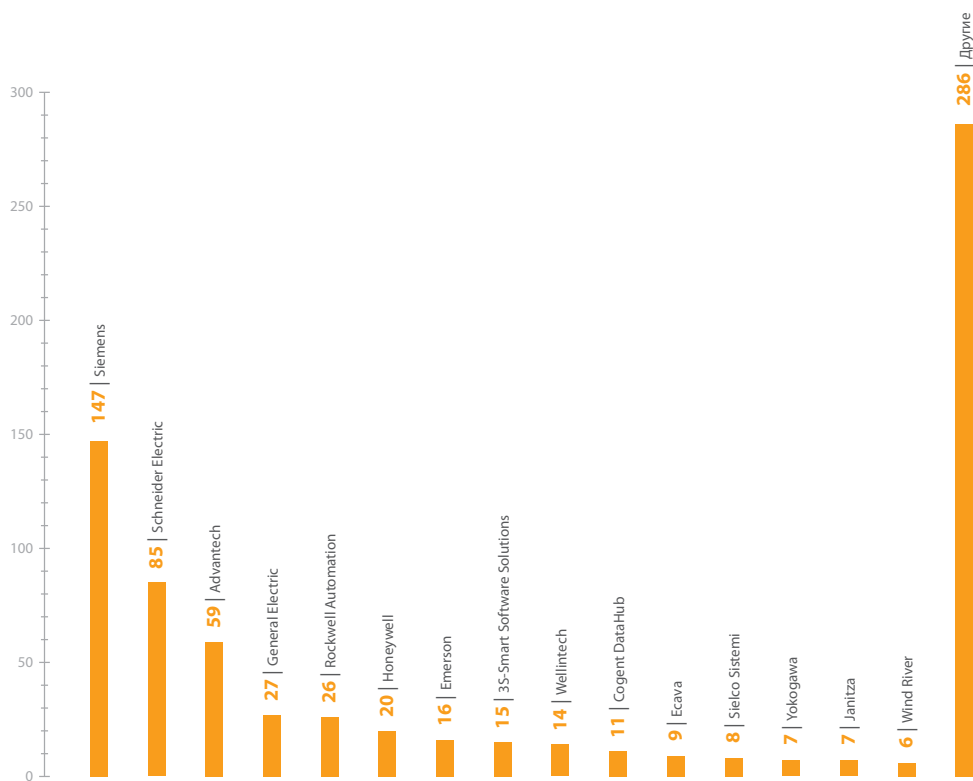


Рис. 2. Количество уязвимостей в компонентах АСУ ТП различных производителей



### 3.3. Уязвимости различных компонентов АСУ ТП

Вопрос классификации компонентов АСУ ТП нельзя назвать тривиальным. В данном исследовании мы объединили типы компонентов. За подробной классификацией можно обратиться к специализированным ресурсам, например к изданию Control<sup>9</sup>.

Наибольшее количество уязвимостей было выявлено в SCADA- и ЧМИ-компонентах, ПЛК/ТУД (RTU), сетевых устройствах промышленного назначения и инженерном программном обеспечении, что также соответствует данным предыдущего отчета за 2012 год.

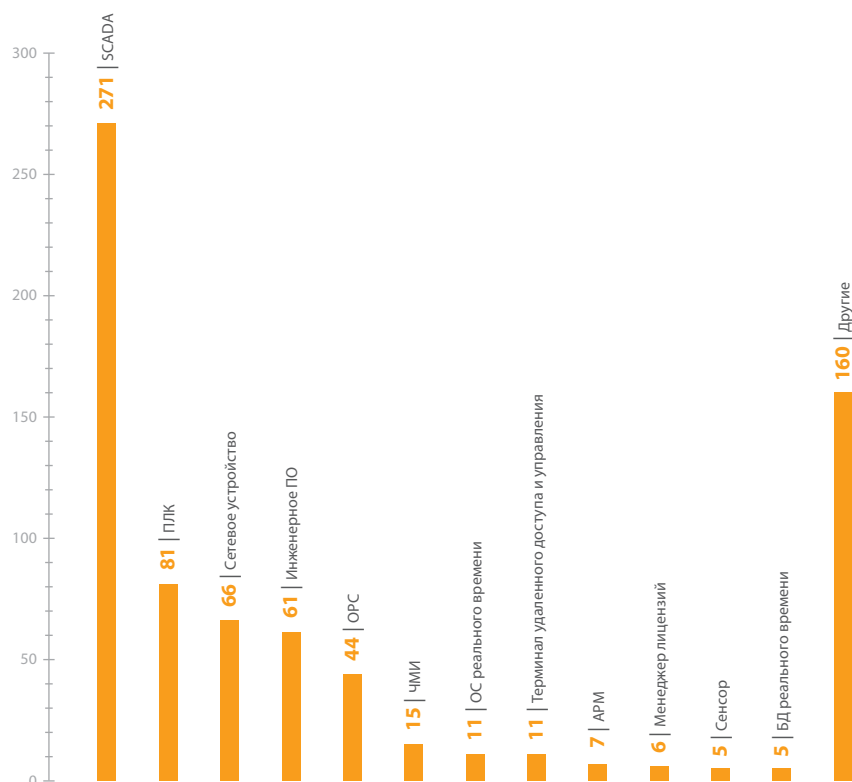


Рис. 3. Уязвимости в различных компонентах АСУ ТП

### 3.4. Степень риска выявленных уязвимостей

Из 743 выявленных уязвимостей практически половина (47%) имеют высокую степень риска.

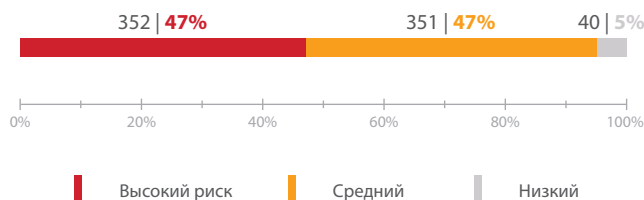


Рис. 4. Распределение уязвимостей по степени риска

<sup>9</sup> [www2.emersonprocess.com/siteadmincenter/PM%20Articles/ControlReadersChoice2014.pdf](http://www2.emersonprocess.com/siteadmincenter/PM%20Articles/ControlReadersChoice2014.pdf)  
[textlab.io/doc/3540422/controlreaderschoice2015](http://textlab.io/doc/3540422/controlreaderschoice2015)

На рис. 5 представлено распределение компонентов АСУ ТП различных производителей по степени риска. В категорию «Другие» снова вошли производители, продукты которых имеют небольшое количество уязвимостей и незначительное распространение.

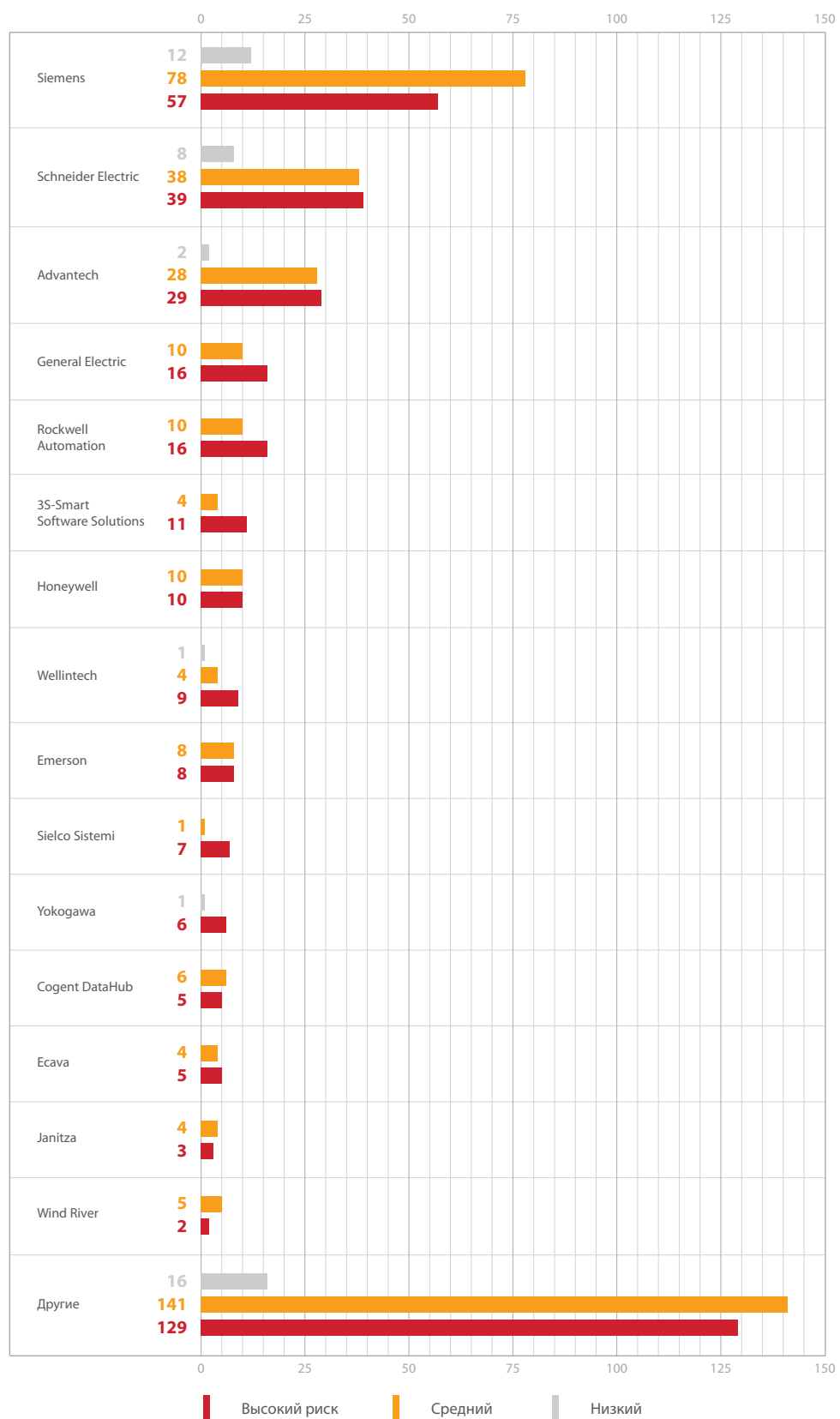


Рис. 5. Уязвимости в компонентах АСУ ТП различных производителей по степени риска

Вектор CVSS предусматривает оценку уровня опасности уязвимости исходя из возможности реализации главных угроз информационной безопасности (нарушения конфиденциальности, целостности и доступности) в результате ее эксплуатации, а также учитывает сложность и условия эксплуатации. Больше половины уязвимостей имеют высокую метрику «Нарушение доступности» (рис. 6).

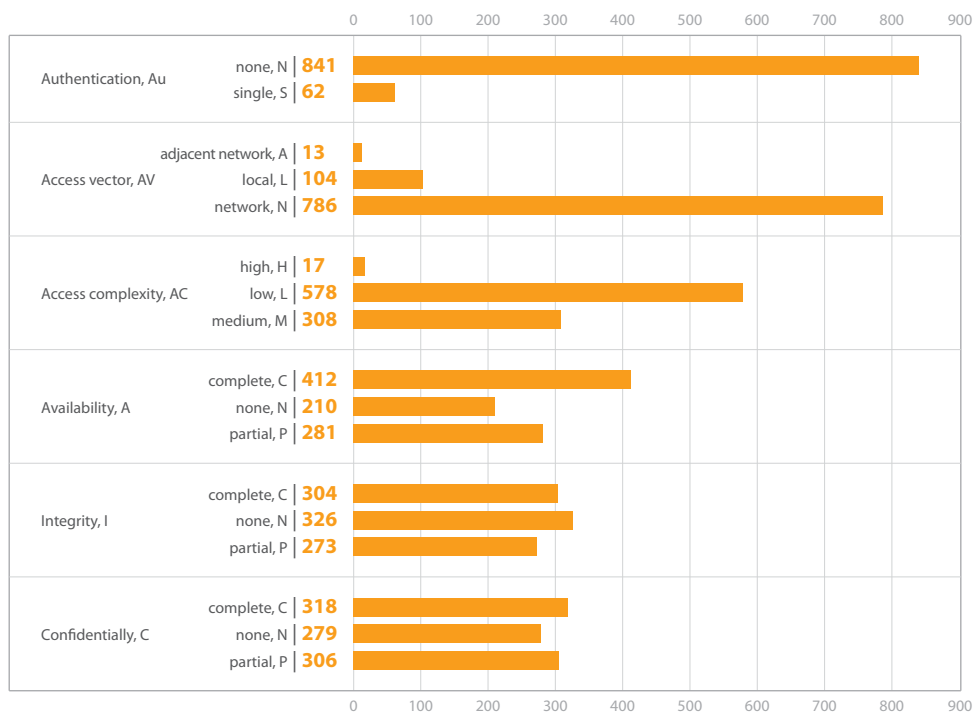


Рис. 6. Количество уязвимостей с теми или иными значениями метрик CVSS

### 3.5. Доля устраненных уязвимостей в компонентах АСУ ТП и возможности для проведения атак

Поскольку данные о процессе устранения уязвимостей не публикуются, в данный раздел была включена информация, полученная Positive Technologies непосредственно от производителей. Подробная информация о выявленных уязвимостях, которые уже устранены производителями, представлена на сайте Positive Technologies<sup>10</sup>.

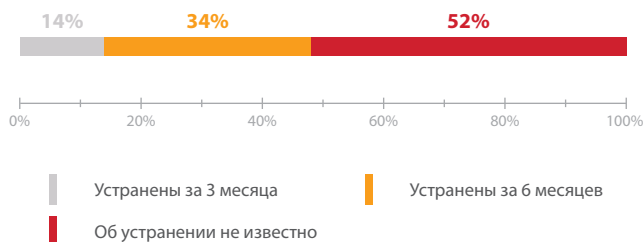


Рис. 7. Доля устраненных уязвимостей в компонентах АСУ ТП

<sup>10</sup> [ptsecurity.ru/research/threatscape](http://ptsecurity.ru/research/threatscape)

По данным 2015 года, лишь 14% уязвимостей были устранены в течение трех месяцев, 34% устранялись более трех месяцев, а оставшиеся 52% ошибок — либо вовсе не исправлены, либо производитель не сообщает о времени устранения.

Вместе с тем в настоящее время только для 5% известных уязвимостей имеются опубликованные эксплойты.

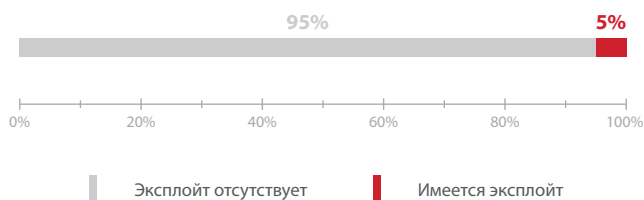


Рис. 8. Доля уязвимостей, имеющих эксплойты

Данный показатель значительно снизился по сравнению с 2012 годом. Это, а также практически неизменное количество уязвимостей, обнаруживаемых в год, связано с тем, что в настоящее время производители оборудования заинтересованы в устранении уязвимостей и взаимодействуют с исследователями в целях оперативного выявления уязвимостей, опираясь на политику ответственного разглашения. Впрочем, следует иметь в виду: столь низкий показатель не свидетельствует о хорошей защищенности систем, поскольку могут существовать неопубликованные эксплойты.

### 3.6. Распределение уязвимостей по типу

Наибольшее количество уязвимостей относятся к таким типам, как отказ в обслуживании (DoS), удаленное выполнение кода (Code Execution) и переполнение буфера (Overflow). Доли основных наиболее распространенных типов уязвимостей представлены на рис. 9 (прочие типы имеют незначительные доли — менее 4% — и потому не представлены).

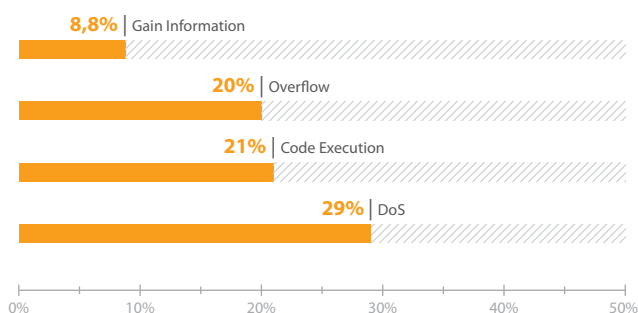


Рис. 9. Распространенные типы уязвимостей компонентов АСУ ТП

Эксплуатация таких уязвимостей злоумышленником может привести к отказу в работе какого-либо оборудования или к его несанкционированной эксплуатации, что, учитывая требования к штатной работе АСУ ТП, недопустимо.

## 4. Распространенность компонентов АСУ ТП в сети Интернет

### 4.1. Распространенность компонентов АСУ ТП

В результате исследования всего было выявлено 158 087 компонентов АСУ ТП, доступных в сети Интернет. Если рассматривать доступные компоненты в зависимости от используемого ими протокола, то было выявлено, что наибольшее количество компонентов АСУ ТП доступно по протоколу HTTP.

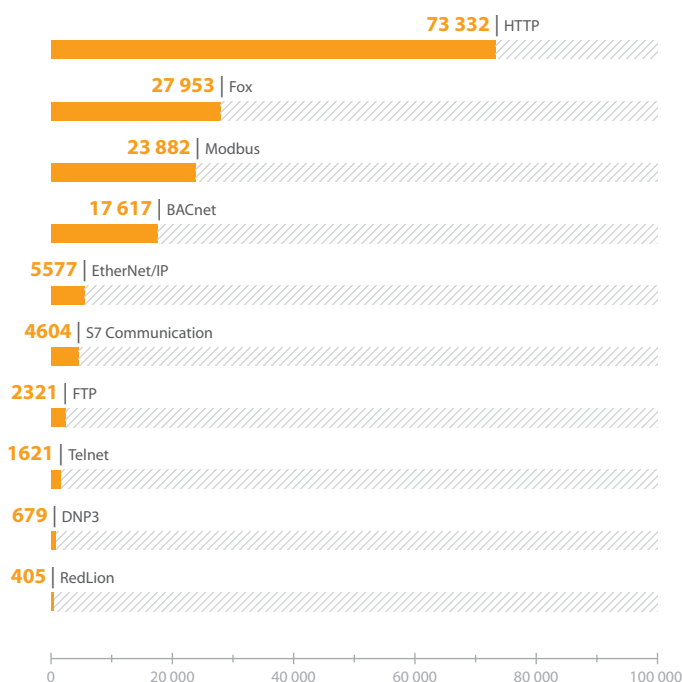


Рис. 10. Используемые протоколы (указано количество компонентов АСУ ТП)

### 4.2. Территориальное распределение компонентов АСУ ТП

Лидером по количеству найденных компонентов с большим отрывом являются США (39%), второе место занимает Германия (12%), затем следуют Франция, Италия и Канада (примерно по 5%). Это, среди прочего, связано с широким распространением современных АСУЗ, которые наиболее популярны в этих странах с общим высоким уровнем автоматизации.

В табл. 1 представлены страны, где компонентов АСУ ТП было выявлено больше всего. Семь из десяти стран в этом списке — из европейского региона. Низкое количество АСУ ТП, обнаруженных в Азии, связано с использованием локальных и малоизвестных на мировом рынке решений. Россия занимает 31 место с 600 доступными компонентами (это менее 1% общего числа найденных компонентов).

Обнаруженные в европейском сегменте сети Интернет компоненты АСУ ТП составляют около половины от общего числа всех найденных компонентов. Около 40% компонентов сосредоточены в Новом Свете, где с большим отрывом лидируют США и Канада. Страны — технологические лидеры ожидаемо имеют высокую концентрацию компонентов АСУ ТП в сети Интернет.

Таблица 1. Топ-10 стран по распространенности АСУ ТП в сети Интернет

Страна	Количество доступных компонентов	Доля в общем числе доступных компонентов
США	61 413	38,85 %
Германия	19 419	12,28 %
Франция	8 577	5,43 %
Италия	8 141	5,15 %
Канада	7 801	4,93 %
Испания	4 627	2,93 %
Австралия	3 233	2,05 %
Швеция	2 897	1,83 %
Нидерланды	2 790	1,76 %
Великобритания	2 679	1,69 %

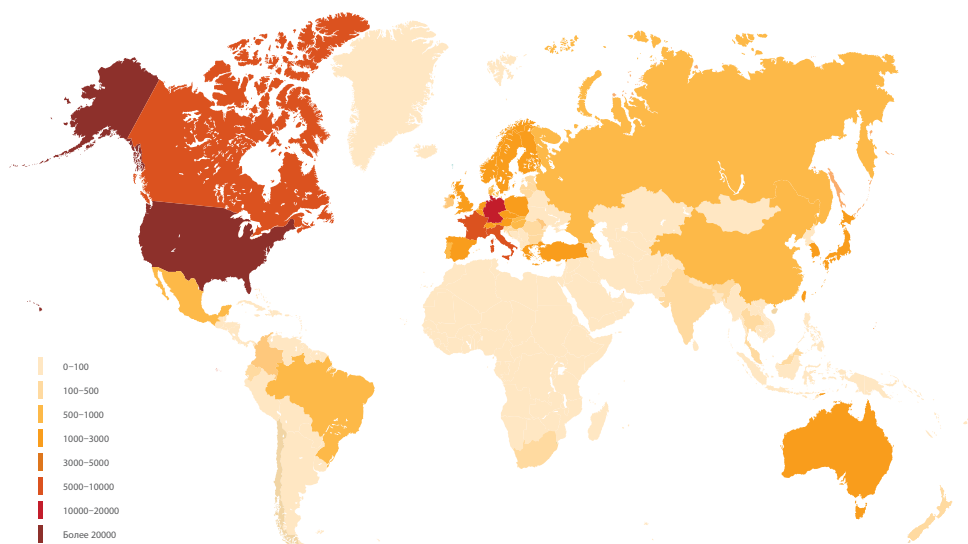


Рис. 11. Число компонентов АСУ ТП, доступных в сети Интернет

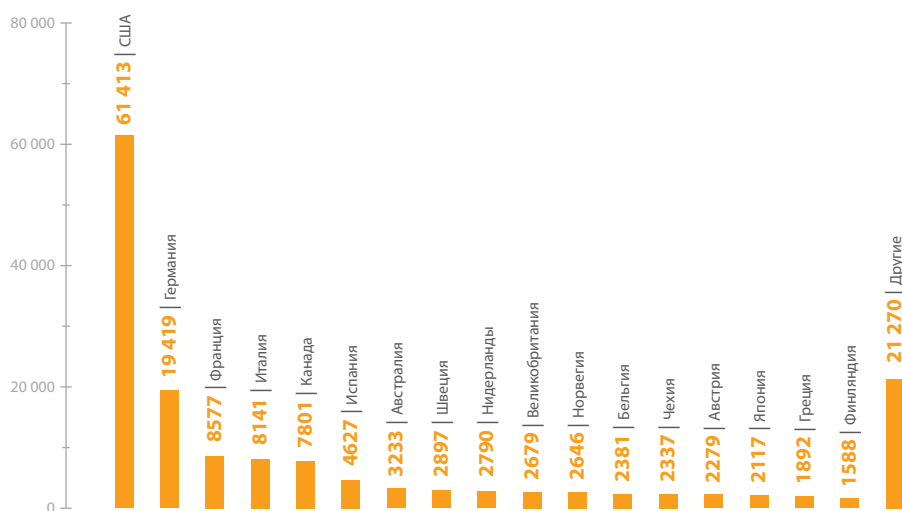


Рис. 12. Число компонентов АСУ ТП, доступных в сети Интернет

На рис. 12 представлено распределения доступных компонентов АСУ ТП в сети Интернет по странам. В категорию «Другие» были отнесены страны с долей не более 1%. При сравнении с результатами исследования 2012 года заметно, что США остались лидером, но второе место заняла не Италия, а с большим отрывом Германия.

### 4.3. Распространенность компонентов АСУ ТП по производителям и продуктам

По распространенности компонентов АСУ ТП лидируют компании Honeywell, SMA Solar Technology, Beck IPC, Siemens и Bosch Security Systems.

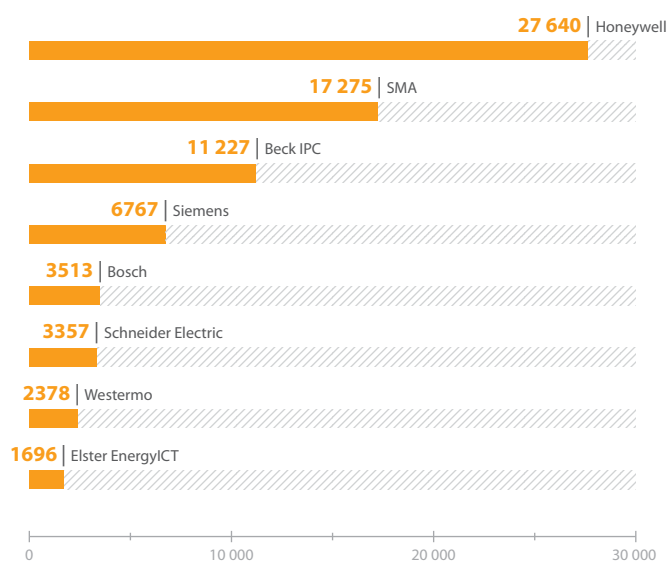


Рис. 13. Распределение компонентов АСУ ТП, доступных в сети Интернет, по производителям

Выпускаемый компанией Honeywell программный продукт Niagara Framework лидирует по количеству доступного в сети Интернет оборудования. Всего было найдено 27 640 таких устройств (17% от общего числа). Кроме того, было обнаружено около 700 различных АСУЗ производства этой компании и 1696 устройств Elster EnergyICT (Honeywell) WebRTU.

Второе место среди производителей и продуктов заняла компания SMA Solar Technology со своим продуктом Sunny WebBox. Компания занимается производством систем для автоматизации зданий и управления электроэнергией. В глобальной сети обнаружилось около 17 300 устройств этой компании (это 11%).

Третье место заняла немецкая компания Beck IPC с устройством IPC@CHIP (доля в 7%).

Четвертое место у Siemens: было найдено 4930 АСУЗ, созданных подразделением Siemens Building Technologies, а также 1840 единиц другого оборудования компании — ПЛК, РСУ и прочего.

На пятом, шестом и седьмом месте компании Bosch (3513 компонентов), Schneider Electric (3360) и Westermo (2378). Следует отметить, что компания Schneider Electric отличается большим разнообразием оборудования, доступного в глобальной сети; например, было найдено 900 ПЛК Modicon M340, 650 ПЛК TWDLCAE40DRF и 360 счетчиков ION6800. А продукты Bosch Security Systems, подразделения компании Bosch, используются, в частности, в аэропорте Мадрид-Барахас в Испании.

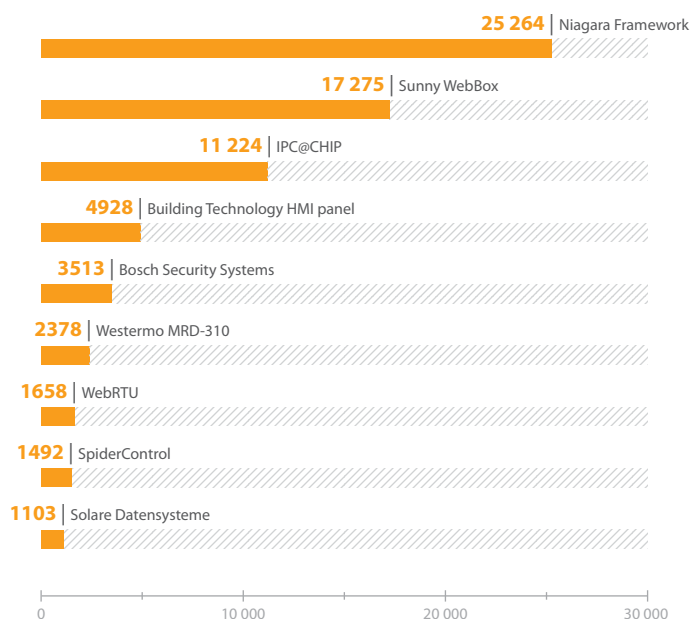


Рис. 14. Количество компонентов АСУ ТП, доступных в сети Интернет

При проведении анализа было также выявлено примерно по 1000 устройств SpiderControl, Sofrel Lacroix S500 и Solare Datensysteme. Были, кроме того, выявлены производители и продукты с долей меньше 1%, а также оборудование, производителя которого выявить не удалось.

Согласно докладу, опубликованному ICS-CERT<sup>11</sup>, наибольшее количество инцидентов в США в 2015 году было выявлено в критически важной инфраструктуре, в том числе в области энергетики. Следует отметить, что при анализе информации о доступности компонентов АСУ ТП доступных в сети Интернет специалисты Positive Technologies определили, что 4893 компонента АСУ ТП, доступных в сети Интернет, применяются в области энергетики, а 51 425 относятся к области автоматизации зданий. Если для сравнения этих данных с исследованием ICS-CERT исключить из рассмотрения данные по автоматизации зданий, доля компонентов, применяющихся в области энергетики и доступных из сети Интернет, будет составлять почти 20% от общего числа. Это говорит об уязвимости одной из ведущих областей хозяйственно-экономической деятельности, нарушение функционирования которой может привести к серьезным последствиям.

Наибольшее количество компонентов, доступных в сети Интернет, в области энергетики было найдено у компаний Honeywell (2168), Schneider Electric (933), Solare Datensysteme (820), SenecIES (256), Nordex (239), Echelon (227) и Electro Industries/GaugeTech (138). Распределение компонентов АСУ ТП среди производителей оборудования представлено на рис. 15. В категорию «Другие» вошли компании с незначительным числом найденных компонентов.

Компания Schneider Electric является вторым по распространенности производителем компонентов в области энергетики; специалисты Positive Technologies обнаружили множество различных модификаций продукта PowerLogic и других электронных устройств. Наиболее распространенными продуктами оказались WebRTU (2130) и Solar-Log (820) компании Solare Datensysteme. Количество найденных компонентов в области энергетики представлено на рис. 16 (в категорию «Другие» вошли чуть менее распространенные компоненты, в том числе и некоторые продукты компании Schneider Electric).

<sup>11</sup> [ics-cert.us-cert.gov/sites/default/files/Annual\\_Reports/Year\\_In\\_Review\\_FY2015\\_Final.pdf](https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_In_Review_FY2015_Final.pdf)



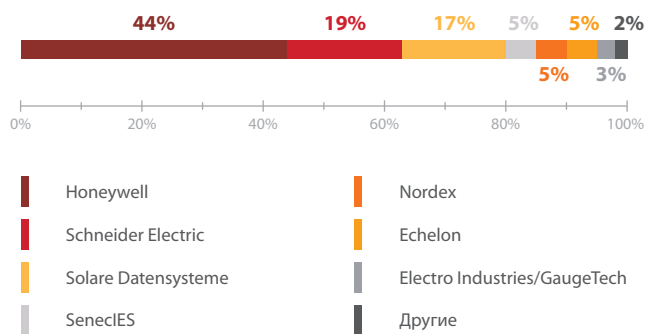


Рис. 15. Компоненты АСУ ТП в области энергетики (по производителям)

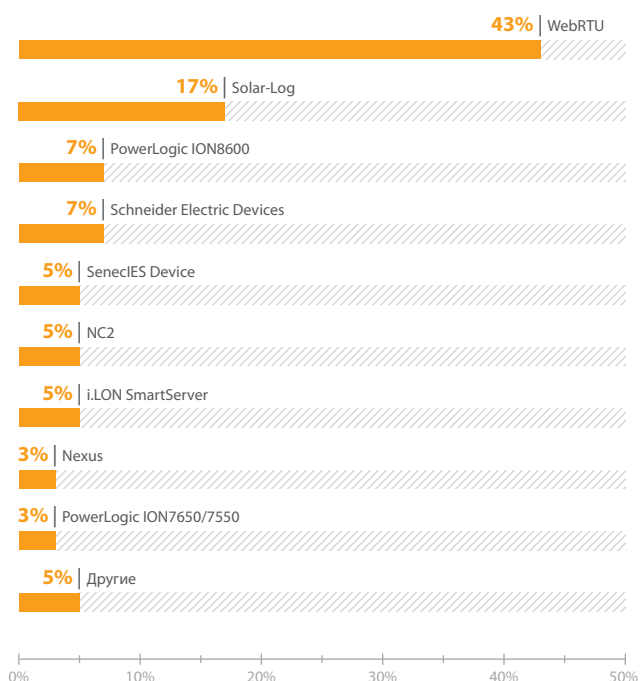


Рис. 16. Доли различных компонентов АСУ ТП в области энергетики

## 4.4. Типы компонентов АСУ ТП

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

Наибольшее количество доступных в сети Интернет продуктов — это устройства, выполняющие функции SCADA/ЧМИ и ПЛК/ТУД (RTU) — 25 250 единиц, что объясняется распространенностью многофункционального продукта Niagara Framework компании Honeywell.

Второе место по распространенности занимают компоненты ПЛК/ТУД и удаленные терминалы. Было найдено 18 233 таких устройств.

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

Компонент АСУ ТП	Найденное количество
ЧМИ/SCADA + ПЛК/ТУД (RTU)	25 264
ТУД/ПЛК	18 233
Электроизмерительный прибор	17 979
ЧМИ/SCADA	13 485
Сетевое устройство	5 016
Сенсор	907
Конвертер интерфейсов	408
Автоматический выключатель	361
Электронное устройство	179
Инвертор	17
РЗА	9
Другие	76 229

Особый интерес представляют такие устройства, как конвертеры интерфейсов, автоматические выключатели, электронные устройства, инверторы и РЗА. Это устройства для управления процессами, связанными с производством и передачей электроэнергии. Компрометация подобных устройств, например РЗА, может привести к потерям электроэнергии или даже к серьезным авариям. Учитывая все более широкое распространение цифровых РЗА и доступность подобных устройств в сети Интернет, вероятность атак на них довольно велика.

## 4.5. Количество уязвимых компонентов АСУ ТП

Среди найденных в сети Интернет компонентов АСУ ТП только около половины можно условно назвать защищенными. Так как при сборе информации пассивными методами не всегда удается определить версию продукта АСУ ТП, то достоверно установить, имеются ли в данных компонентах известные уязвимости, не всегда представляется возможным. Также стоит учитывать, что отсутствие известных уязвимостей не позволяет назвать систему защищенной — при отсутствии необходимых мер защиты, в особенности, собственно, при доступности такой системы из глобальной сети.

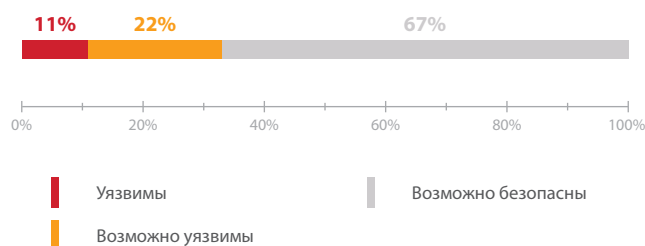


Рис. 17. Доля уязвимых и безопасных компонентов АСУ ТП в сети Интернет

## Заключение

Проведенное исследование показывает, что количество уязвимых компонентов АСУ ТП из года в год не снижается. Практически половина выявленных уязвимостей имеет высокую степень риска. Наибольшее количество уязвимостей было найдено в продуктах самых известных производителей. Наиболее уязвимыми и вместе с тем распространенными компонентами являются SCADA-системы. Наибольшее количество компонентов, доступных в сети Интернет, было обнаружено в странах, в которых системы автоматизации развиты лучше всего.

Большинство компонентов, которые доступны в сети Интернет, являются многофункциональными устройствами. Повсеместно в АСУ ТП используются словарные пароли и пароли по умолчанию, что позволяет без труда получить к ним доступ и перехватить управление.

Полученные данные говорят об отсутствии адекватной защиты компонентов АСУ ТП. Даже минимальные превентивные меры защиты, такие как использование сложных паролей и отключение компонентов АСУ ТП от сети Интернет, позволят в значительной степени снизить вероятность проведения атак, несущих заметные последствия.

---

### О компании

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована «Газпромом» и ФСТЭК. Более 3000 организаций из 30 стран 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 телекомов. В 2013 году компания заняла третье место на российском рынке ПО для безопасности и стала лидером по темпам роста на международном рынке систем управления уязвимостями. В 2015 году Gartner назвал Positive Technologies «визионером» в своем рейтинге Magic Quadrant for Web Application Firewalls.