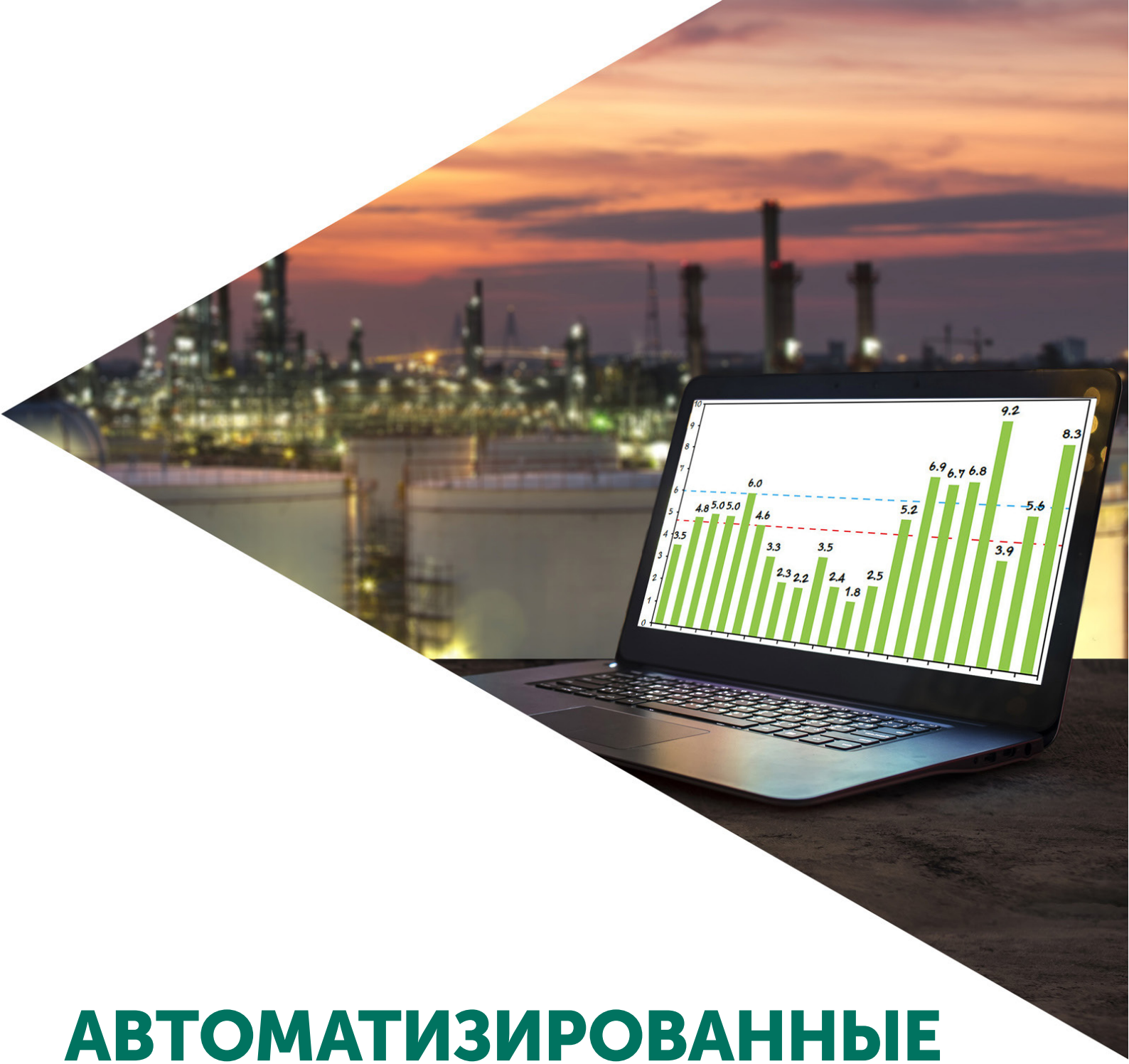

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ И ИХ ДОСТУПНОСТЬ ЧЕРЕЗ ИНТЕРНЕТ

Оксана Андреева, Сергей Гордейчик, Глеб Грицай, Ольга Кочетова, Евгения Поцелуевская, Сергей Сидоров, Александр Тиморин

Оглавление

1 Введение 3
1.1 Общие сведения 3
1.2 Подход к анализу 3
2 Основные результаты исследования 4
3 Доступность АСУ ТП 5
3.1 Общие сведения 5
3.2 Доступность по производителям 5
3.3 Доступность различных типов компонентов АСУ ТП 6
3.4 Протоколы 6
3.5 Страны и отрасли 7
3.6 Уязвимые компоненты АСУ ТП 12
4 Заключение 15

1 Введение

1.1 Общие сведения

Автоматизированные системы управления технологическими процессам (АСУ ТП) — повсюду: они используются в электроэнергетике, водоснабжении и канализации, нефтегазовой промышленности, на транспорте, в химической, фармацевтической, целлюлозно-бумажной и пищевой отраслях, а также на предприятиях с дискретным производством (например, выпускающих автомобили, космические аппараты или товары длительного пользования). «Умные» города, дома и автомобили, медицинские системы — в основе всего этого лежат АСУ ТП.

С каждым годом растет число компонентов АСУ ТП, доступных через интернет. И это делает их более уязвимыми для атак. Поскольку первоначально многие решения и протоколы, используемые в АСУ ТП, проектировались для изолированных сред, а также без учета будущих проблем безопасности, такая доступность часто дает злоумышленникам различные возможности для воздействия на инфраструктуру АСУ ТП вследствие отсутствия необходимых средств обеспечения безопасности. Более того, некоторые компоненты АСУ ТП и сами уязвимы. Впервые информация об этом появилась в 1997 году — тогда были опубликованы сведения всего о двух уязвимостях. С тех пор количество известных уязвимостей значительно выросло. В частности, за последние пять лет оно выросло в десять раз — с 19 в 2010 году до 189 в 2015-м.

Тщательно разработанные сложные атаки на системы АСУ ТП уже не новость. Взять хотя бы инцидент, произошедший в 2015 году в Ивано-Франковске (Украина), когда около половины домов остались без электричества из-за кибератаки на энергокомпанию «Прикарпатьеоблэнерго» — одну из многочисленных жертв APT-кампании BlackEnergy[1].

Еще один примечательный инцидент, информация о котором была опубликована в бюллетене Verizon Data Breach Digest[2], произошел в 2015 году — тогда была атакована инфраструктура АСУ ТП коммунальной компании Kemuri Water Company. В ходе атаки злоумышленникам удалось проникнуть в систему управления компании и изменить количество химических реагентов, применяемых в ходе очистки воды, подаваемой в водопровод. Внедрение осуществлялось через уязвимую, доступную извне систему, которая была предназначена для управления программируемыми логическими контроллерами (ПЛК), регулирующими работу вентилей и трубопроводов, через которые в систему подавалась вода и реагенты для очистки.

В 2015 году имели место и другие инциденты с АСУ ТП — например, атаки на сталелитейный завод в Германии или на аэропорт им. Фредерика Шопена в Варшаве[3].

В настоящем исследовании мы представляем обзор текущей общемировой ситуации в области безопасности АСУ ТП относительно уязвимостей и уязвимых компонентов АСУ ТП, доступных через интернет.

1.2 Подход к анализу

Исследование посвящено доступности автоматизированных систем управления через интернет. Мы применили пассивный подход к анализу. Для идентификации АСУ ТП при поиске в системах Shodan и Censys мы использовали базу сигнатур, содержащую около 2000 записей и позволяющую определить производителей продуктов и их версии по баннерам.

---

[1] https://securelist.ru/blog/issledovaniya/27903/pri-apt-atakax-blackenergy-v-ukraine-primenyalsya-celevoj-fishing-s-ispolzovaniem-word-dokumentov/

[2] http://www.verizonenterprise.com/verizon-insights/data-breach-digest/2016/

[3] https://securelist.ru/analysis/ksb/27466/kaspersky-security-bulletin-2015-razvitie-ugroz-v-2015-godu/

2 Основные результаты исследования

Были сделаны следующие выводы.

- **Через интернет доступно значительное число компонентов АСУ ТП**. В поисковой системе Shodan было обнаружено 220 558 компонентов АСУ ТП, размещенных на 188 019 хостах в 170 странах. Большинство хостов с компонентами АСУ ТП, к которым возможен удаленный доступ, находятся в США (30,5%) и Европе. Среди европейских стран первое место занимает Германия (13,9%), за ней следует Испания (5,9%). Доступные системы созданы 133 различными производителями. Наиболее распространены АСУ ТП Tridium (11,1%), Sierra Wireless (8,1%) и Beck IPC (6,7%).
- **Компоненты АСУ ТП, к которым возможен удаленный доступ, используют незащищенные протоколы передачи данных**. Используется несколько протоколов, являющихся открытыми и незащищенными по своей природе, такие как HTTP, Niagara Fox, Telnet, EtherNet/IP, Modbus, BACnet, FTP, Omron FINS, Siemens S7 и многие другие. Они применяются на 172 338 различных хостах, что соответствует 91,6% всех обнаруженных АСУ ТП, доступных через внешние сети. Это дает злоумышленникам дополнительные возможности взлома устройств путем проведения атак типа Man-in-the-Middle («человек посередине»).
- **Через внешние сети доступно большое число уязвимых АСУ ТП**. Мы обнаружили 13 033 уязвимости на 11 882 хостах (это 6,3% всех хостов, на которых размещены компоненты, доступные из внешних сетей). Наиболее распространенные из обнаруженных уязвимостей — CVE-2015-3964 (жестко прописанные учетные данные в системе управления солнечными батареями Sunny WebBox — Sunny WebBox Hard-Coded Credentials), а также критические уязвимости CVE-2015-1015 и CVE-2015-0987 в ПЛК Omron CJ2M. Сопоставление этих результатов со статистикой использования незащищенных протоколов позволило нам оценить общее число уязвимых хостов с компонентами АСУ ТП — 172 982 хоста (92%).
- **Проблема затрагивает различные отрасли**. Мы обнаружили, что не менее 17 042 компонентов АСУ ТП на 13 698 различных хостах в 104 странах, по всей вероятности, принадлежат крупным компаниям, и можно с высокой долей уверенности предположить, что доступность этих компонентов через интернет сопряжена с высоким уровнем риска. Нам удалось выявить 1433 крупные организации из числа владельцев данных АСУ ТП, в том числе принадлежащие к следующим отраслям: электроэнергетика, аэрокосмическая, транспортная (включая аэропорты), нефтегазовая, металлургическая, химическая, сельскохозяйственная и автомобильная отрасли, коммунальные услуги, производство пищевых продуктов и напитков, строительная отрасль, индустрия систем хранения жидкостей и сжиженных газов, «умные» города и производители АСУ ТП. Среди идентифицированных владельцев АСУ ТП, доступных через внешние сети, есть также исследовательские и образовательные учреждения, государственные организации (включая полицию), медицинские центры, финансовые организации, курорты, гостиницы, музеи, библиотеки, церкви и различные предприятия малого бизнеса. Число доступных через внешние сети хостов АСУ ТП, которые, вероятно, принадлежат крупным организациям, составляет 12 483 (91,1%), причем 453 хоста (3,3%) содержат критические уязвимости, включая хосты, принадлежащие энергетическим, транспортным, газовым и инженерно-производственным компаниям, а также производителям пищевых продуктов и напитков.

Все эти результаты соответствуют нижней границе оценки, и в действительности число компонентов АСУ ТП, доступных из внешних сетей, может быть значительно выше.

3 Доступность АСУ ТП

3.1 Общие сведения

Доступность компонентов АСУ ТП в интернете — это серьезная угроза безопасности, ведь в большинстве случае они проектируются с учетом физической изоляции соответствующих сетей. Поэтому на таких устройствах порой нет даже базовых средств защиты.

На основе информации из поисковой системы Shodan мы обнаружили целых **220 558 компонентов АСУ ТП**, доступных в интернете и расположенных **на 188 019 хостах в 170 странах**. В данном разделе описываются основные выводы по этим системам с внешним доступом.

3.2 Доступность по производителям

Наиболее распространены АСУ ТП от таких производителей, как **Tridium** (24 446 сервисов — 11,1%), **Sierra Wireless** (17 908 сервисов — 8,1%) и **Beck IPC** (14 837 сервисов — 6,7%). В категорию «Прочие» входят 115 производителей, включая Advantech, ABB, Nordex, Honeywell, Emerson и General Electric.

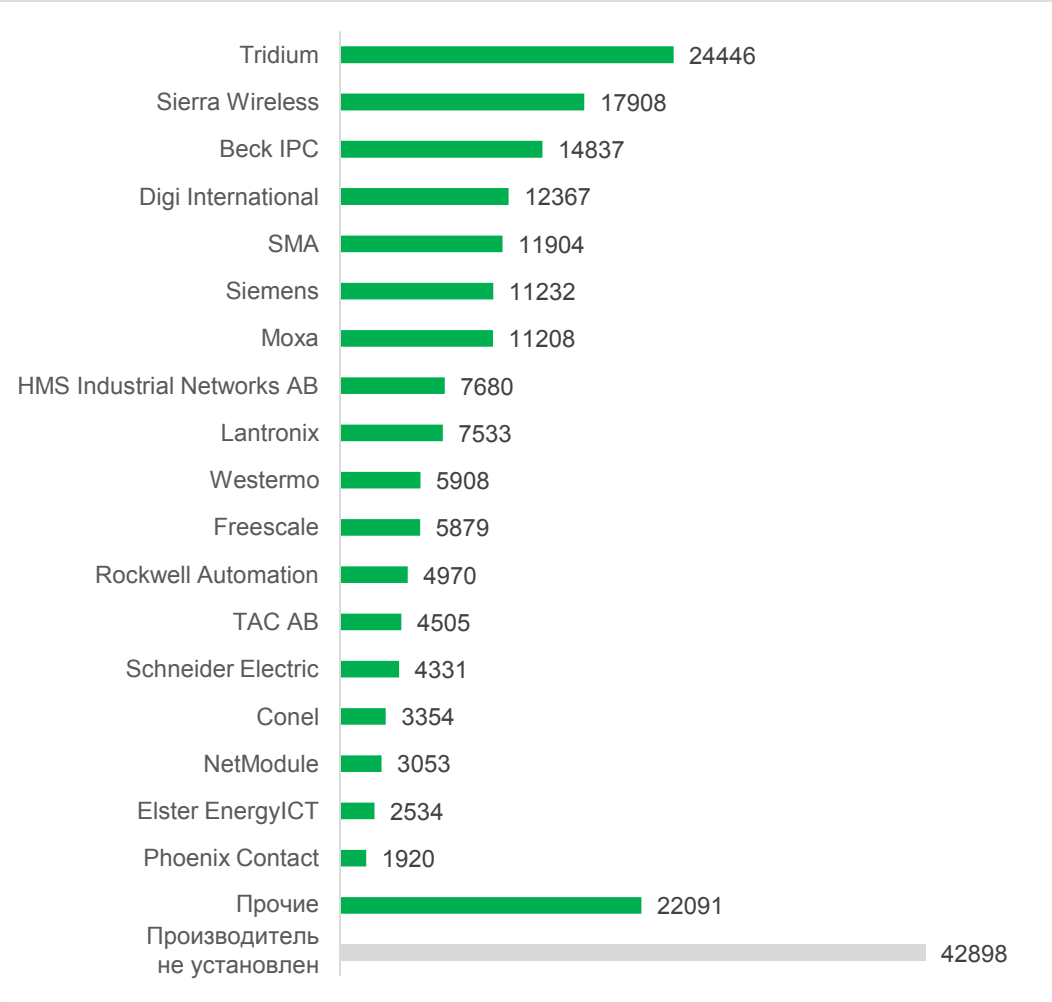

Рисунок 1. Доступность АСУ ТП по производителю

3.3 Доступность различных типов компонентов АСУ ТП

Среди самых распространенных типов доступных компонентов — **промышленные сетевые устройства**: 61 335 сервисов — 27,8%, включая 41 968 промышленных маршрутизаторов и 12 024 промышленных шлюза, **ПЛК** (33 080 сервисов — 14,9%) и **SCADA** (22 624 сервиса — 10,3%). 18,7% всех удаленно доступных сервисов удалось классифицировать как компоненты АСУ ТП (с помощью протоколов или производителей), но установить точный тип устройств путем одного пассивного анализа баннеров невозможно.

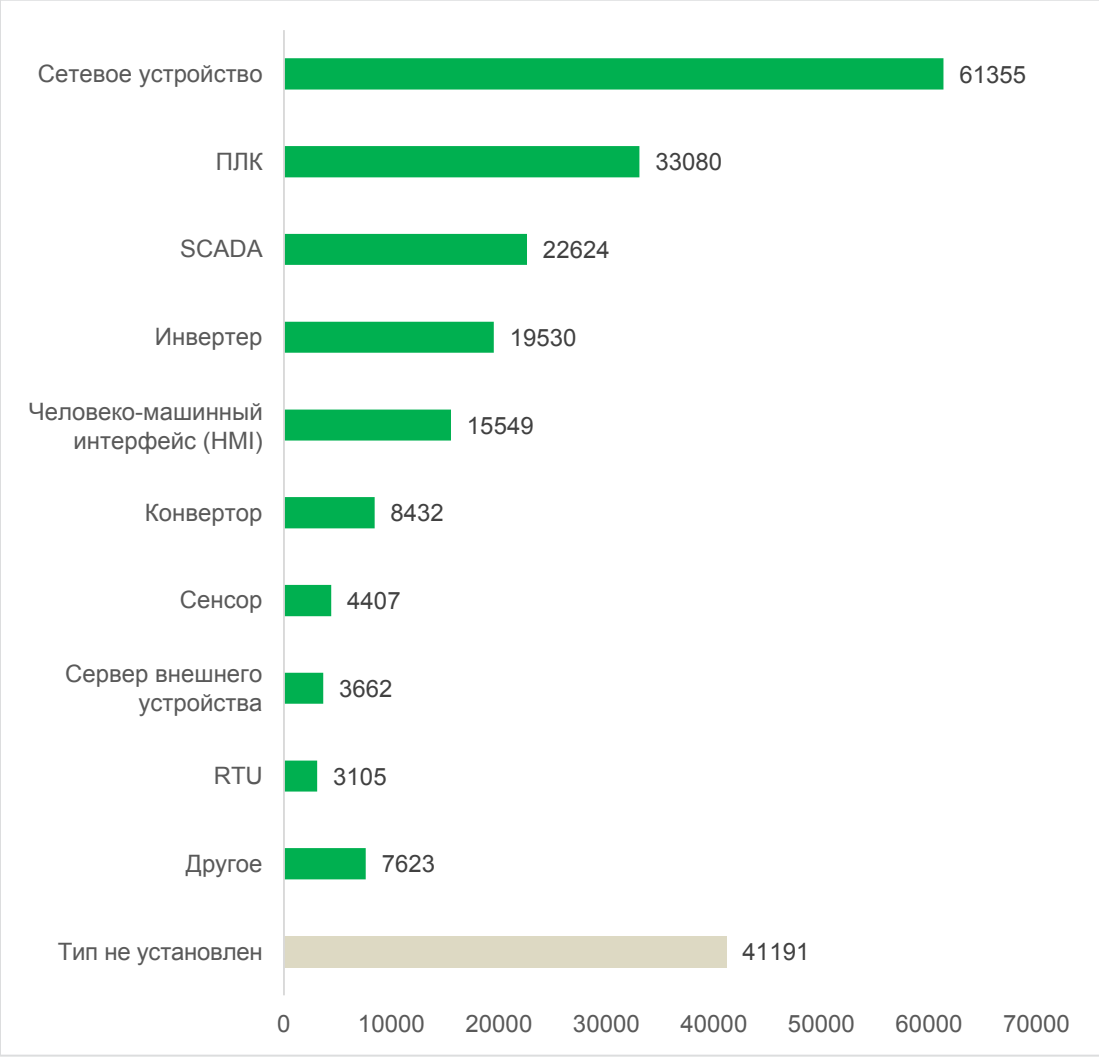

Рисунок 2. Доступность компонентов АСУ ТП

3.4 Протоколы

Обнаруженные компоненты АСУ ТП доступны через различные протоколы. Во многих случаях на одном хосте компонентами АСУ ТП используется несколько различных протоколов. Наиболее распространенные из них: HTTP (116 900 доступных сетевых сервисов — 53%), Telnet (29 586 сервисов — 13,4%), Niagara Fox (20 622 доступных сервиса — 9,3%), SNMP (16 752 сервиса — 7,6%) и Modbus (16 233 сервиса — 7,4%).

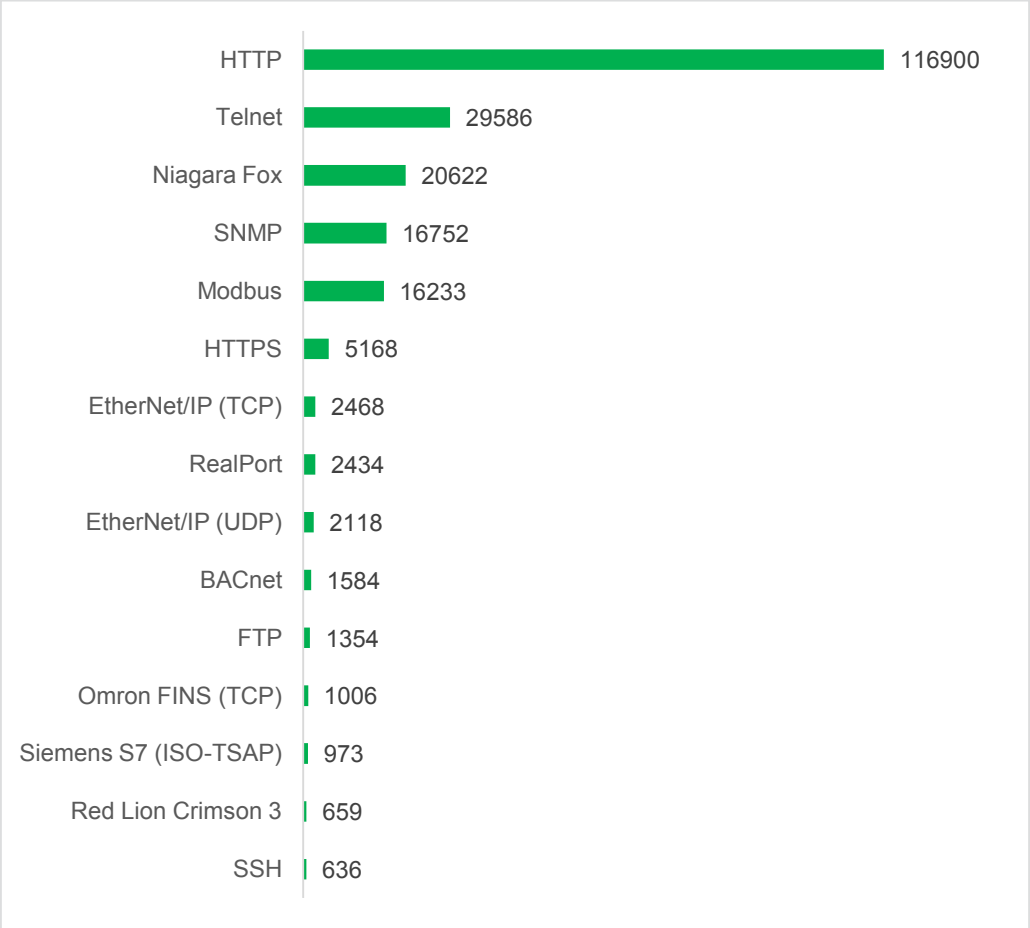

Рисунок 3. 15 основных протоколов, используемых компонентами АСУ ТП с внешним доступом

Помимо того, что доступность компонентов АСУ ТП в интернете — само по себе слабое место в системе безопасности, **большинство используемых протоколов (88,8%) имеют открытую и потому незащищенную архитектуру**: HTTP, Niagara Fox, Telnet, EtherNet/IP, Modbus, BACnet, FTP, Omron FINS, Siemens S7 и многие другие. Незащищенные протоколы применяются на **172 338 различных хостах, что соответствует 91,6%** всех обнаруженных АСУ ТП, доступных через внешние сети. Это дает злоумышленникам дополнительные возможности взлома устройств путем проведения атак типа Man-in-the-Middle («человек посередине»).

3.5 Страны и отрасли

Большинство хостов с компонентами АСУ ТП, к которым возможен удаленный доступ, находятся в **США** (57 417 хостов — 30,5%) и Европе. Среди европейских стран первое место занимает **Германия** (26 142 хоста — 13,9%), за ней следуют Испания (11 264 хоста — 5,9%) и Франция (10 578 хостов — 5,6%).

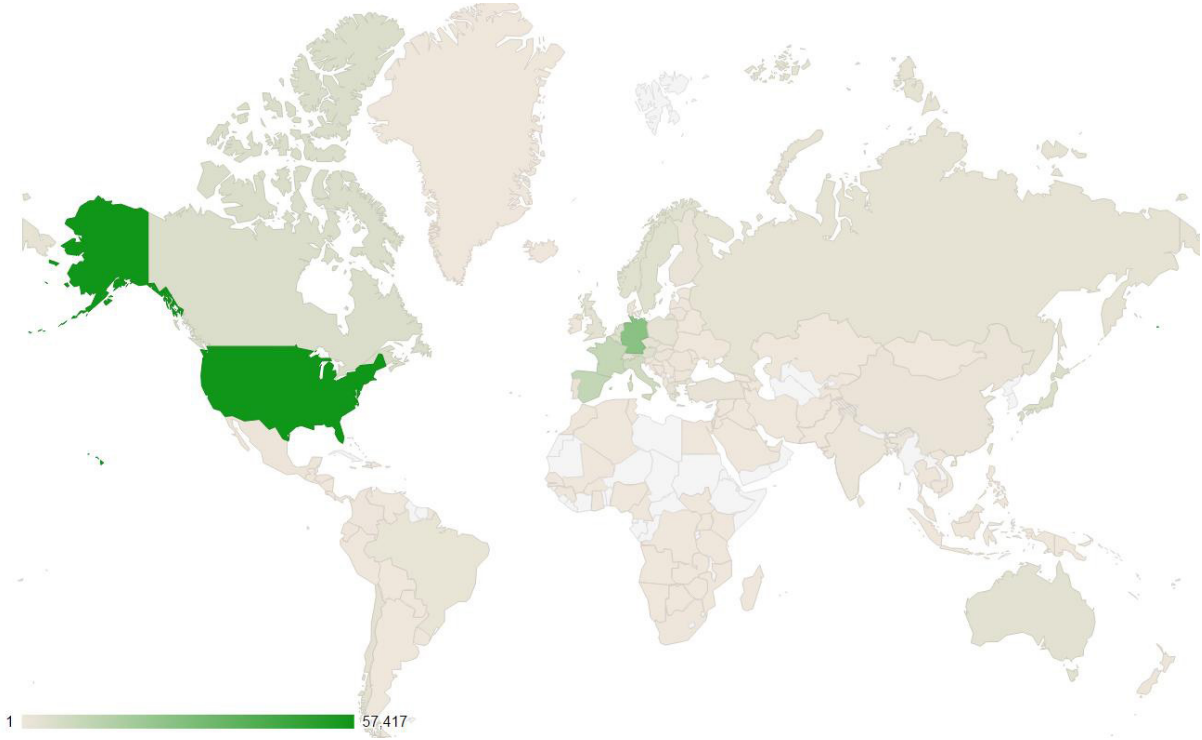

Рисунок 4. Доступность АСУ ТП по стране

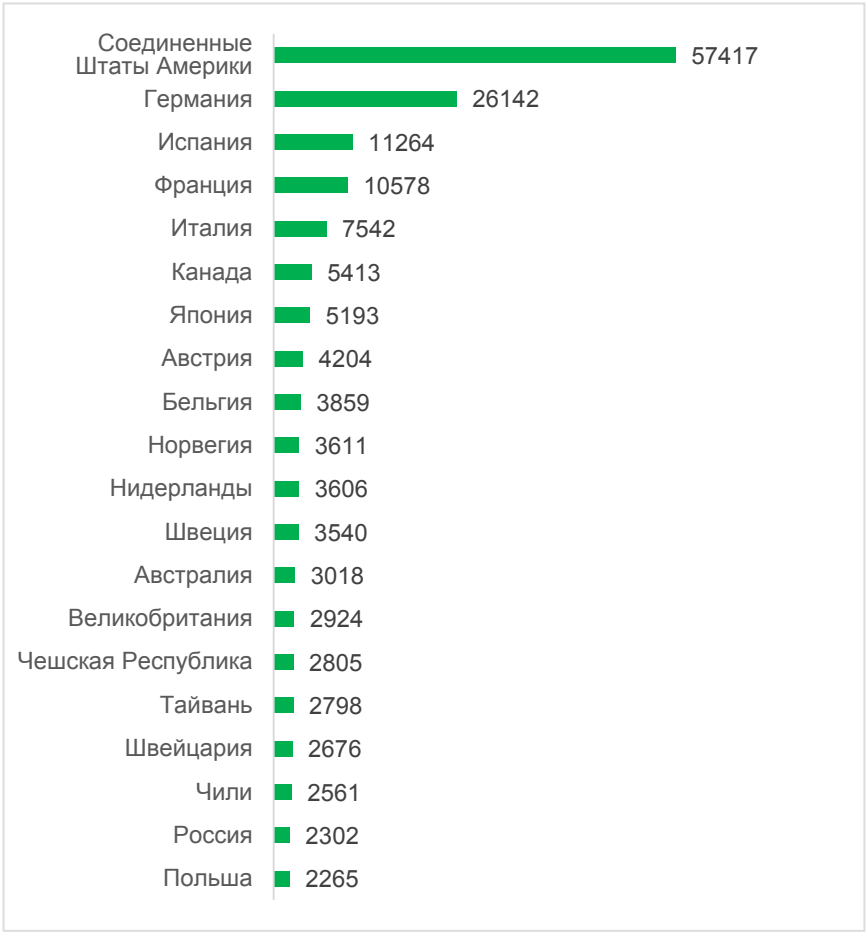

Рисунок 5. Доступность АСУ ТП по стране (первые 20)

Подобная статистика, возможно, связана с более высокой степенью развития технологий в США и европейских странах. Анализ отношения числа хостов с установленными компонентами АСУ ТП к общему числу удаленно доступных хостов в стране (по данным Shodan) показывает иную картину: ведущие позиции занимают **Новая Каледония** (0,547%), **Бельгия** (0,475%) и **Норвегия** (0,458%). В этом рейтинге США находятся на 34-м месте, а Германия — на 21-м.

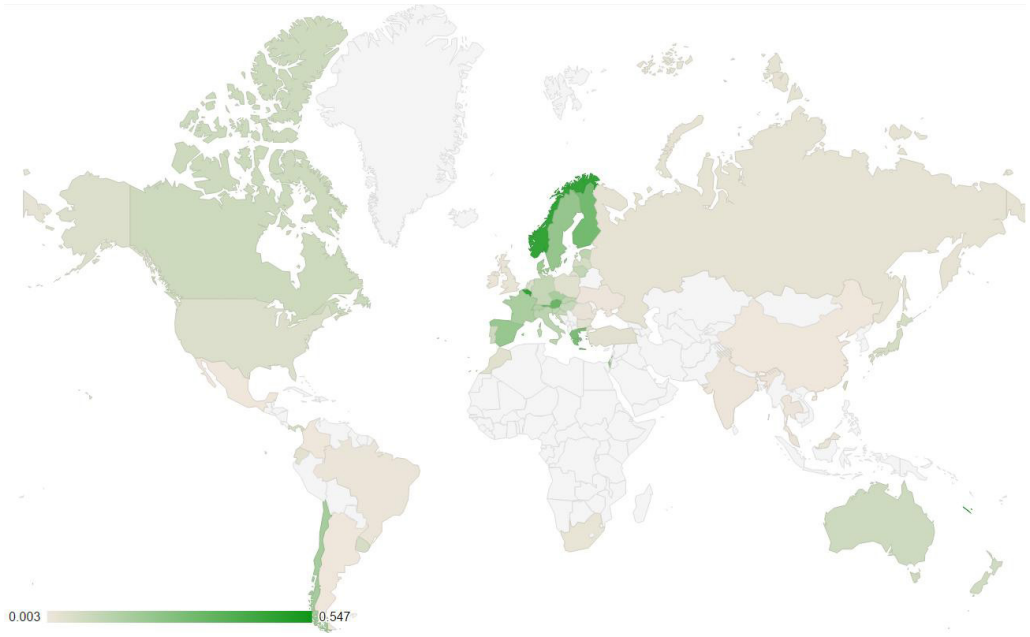

Рисунок 6. Доступность АСУ ТП по стране (соотношение доступных хостов АСУ ТП и общего числа доступных хостов)

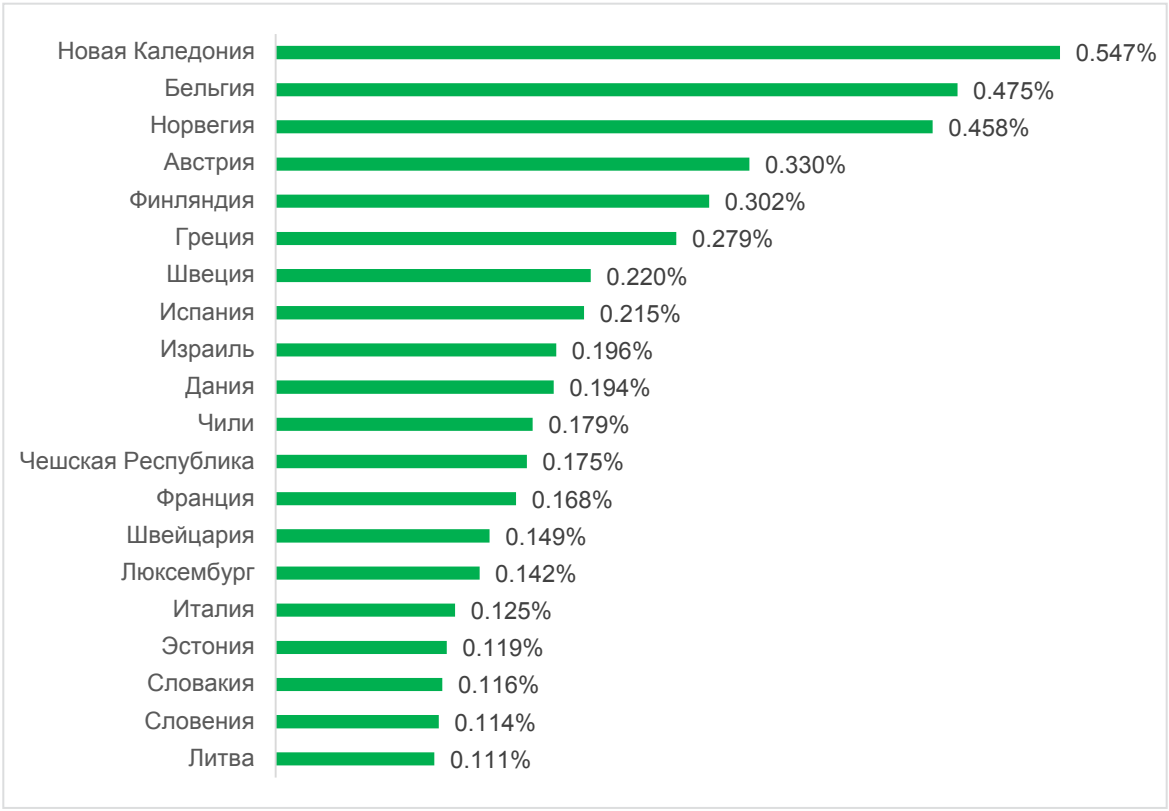

Рисунок 7. Первые 20 доступных АСУ ТП по стране (соотношение доступных хостов АСУ ТП и общего числа доступных хостов

Про большинство удаленно доступных хостов АСУ ТП нельзя точно сказать, кем они используются: домашними пользователями, небольшими и средними компаниями или крупными предприятиями. Мы проанализировали результаты WHOIS для публичных IP-адресов АСУ ТП и обнаружили следующее:

- Как минимум 87,7% IP-адресов (164 905) зарегистрировано на поставщиков телекоммуникационных услуг (включая сотовые и спутниковые сети), поэтому мы не смогли определить их реальных владельцев.
- Как минимум 3,1% хостов (5828) относятся к исследовательским и образовательным учреждениям: университетам, колледжам, школам. Доступные компоненты АСУ ТП могут поддерживать инфраструктуру соответствующих зданий (электричество, кондиционирование воздуха и др.). Однако возможно, что эти компоненты входят в тестовые системы для исследовательских целей.
- Среди прочих пользователей нам удалось выявить 1433 крупные организации, в том числе принадлежащие к следующим отраслям: **электроэнергетика, аэрокосмическая, транспортная (включая аэропорты), нефтегазовая, металлургическая, химическая, сельскохозяйственная и автомобильная отрасли, коммунальные услуги, производство пищевых продуктов и напитков, строительная отрасль, индустрия систем хранения жидкостей и сжиженных газов, «умные» города и производители АСУ ТП**.
- Среди идентифицированных владельцев АСУ ТП, доступных через внешние сети, есть также государственные организации (включая полицию), медицинские центры, финансовые организации, курорты, гостиницы, музеи, библиотеки, церкви и различные предприятия малого бизнеса.

Чтобы узнать, сколько систем могут использоваться большими организациями (в дополнение к тем, владельцы которых были установлены), мы подготовили неисчерпывающий список компонентов АСУ ТП промышленного класса, которые вряд ли принадлежат малым компаниям ввиду своих особенностей и стоимости, а затем добавили этот критерий в наш анализ. В результате мы обнаружили, что **не менее 17 042 компонентов АСУ ТП на 13 698 различных хостах в 104 странах, по всей вероятности, принадлежат крупным компаниям**. Можно с высокой долей уверенности предположить, что доступность этих компонентов через интернет сопряжена с высоким уровнем риска. Однако реальное число, возможно, намного выше, поскольку многие решения АСУ ТП, не вошедшие в контрольный список, могут также использоваться большими организациями.

В тройку стран-лидеров по доступным компонентам АСУ ТП, вероятнее всего, принадлежащих предприятиям, входят **США** (2994 хоста — 21,9%), **Франция** (1331 хост — 9,7%) и **Италия** (1100 хостов — 8%).

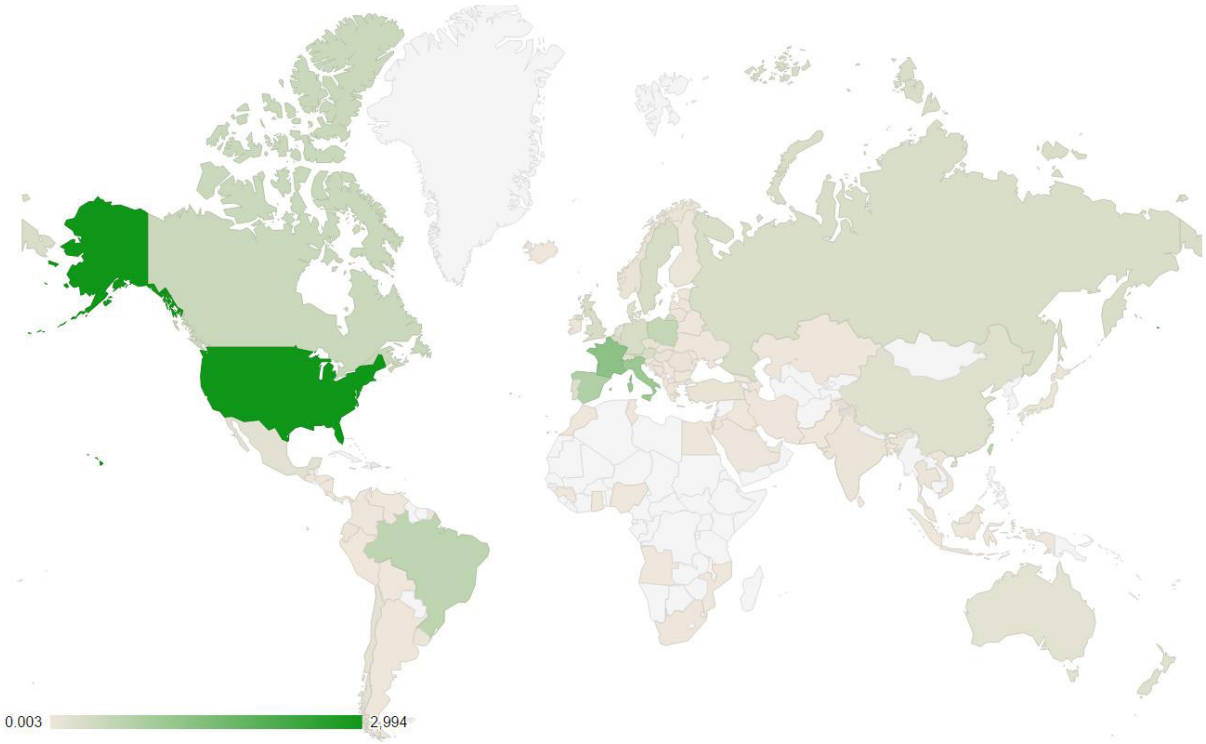

Рисунок 8. Страны с доступными компонентами АСУ ТП корпоративного уровня (примерная нижняя граница)

Рисунок 9. Первые 20 стран с доступными компонентами АСУ ТП корпоративного уровня (примерная нижняя граница)

Наиболее распространенные системы, относящиеся к корпоративному сегменту, принадлежат следующим производителям: **Moxa** (5057 сервисов — 29,7%), **Siemens** (3559 — 20,9%), **Rockwell Automation** (2383 — 13,9%) и **Schneider Electric** (2107 — 12,4%).

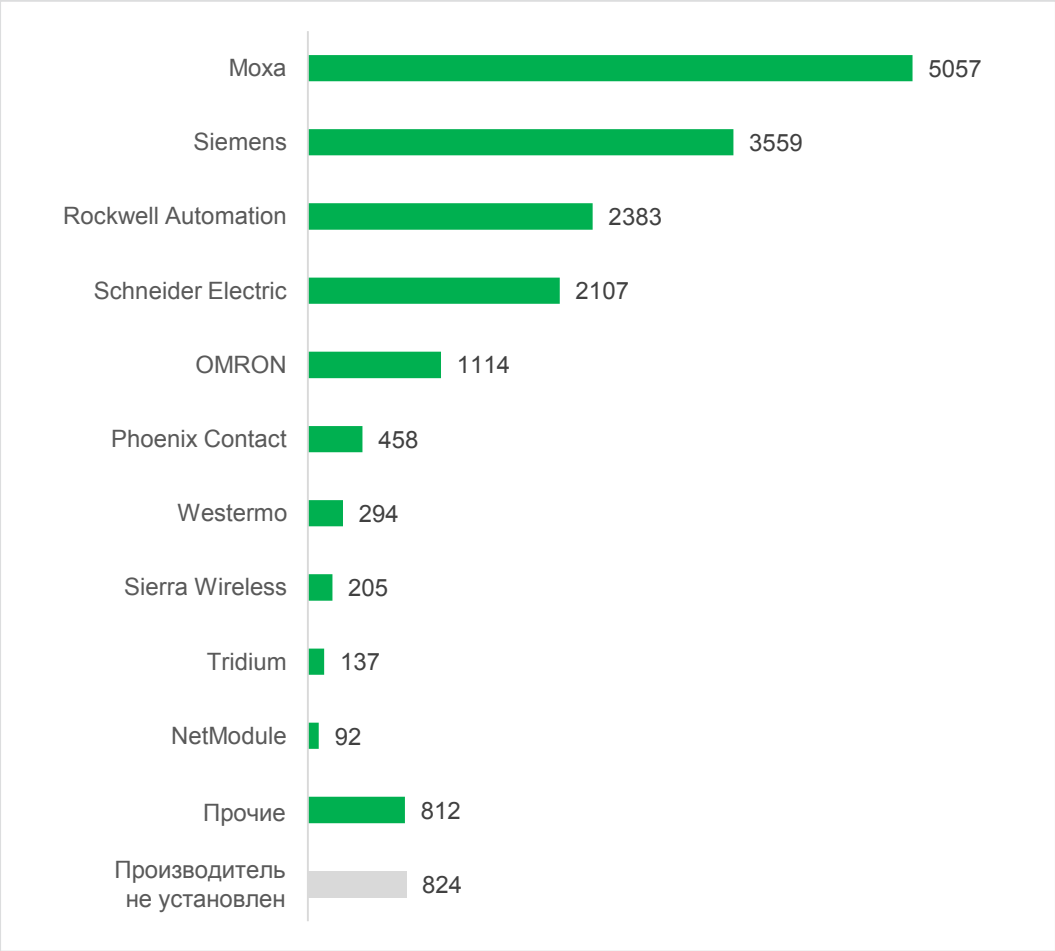

Рисунок 10. Первые 10 производителей АСУ ТП в корпоративном сегменте

3.6 Уязвимые компоненты АСУ ТП

На основе информации от баннеров компонентов АСУ ТП мы проверили эти ресурсы на предмет известных уязвимостей в соответствующих версиях ПО и оборудования. Всего **мы обнаружили 13 033 уязвимости на 11 882 хостах (это 6,3% всех хостов**, на которых размещены обнаруженные компоненты, доступные из внешних сетей). Наиболее распространенные из обнаруженных уязвимостей:

- жестко прописанные учетные данные в системе управления солнечными батареями Sunny WebBox — Sunny WebBox Hard-Coded Credentials (CVE-2015-3964), найденные на 11 904 хостах. У этого решения для управления средними и крупными солнечными электростанциями есть жестко прописанные пароли, благодаря которым гораздо легче получить полный доступ к системе при удаленной атаке.

Уязвимости CVE-2015-1015 и CVE-2015-0987 в ПЛК Omron CJ2M были обнаружены всего на 342 устройствах. В этих устройствах используется восстанавливаемый формат для хранения паролей в файлах объектов на картах памяти Compact Flash. Так, первая из упомянутых уязвимостей упрощает локальный доступ к конфиденциальной информации путем чтения файла. Вторая уязвимость заключается в следующем: чтобы разблокировать ПЛК для изменения, пароль передается открытым текстом,

становясь легкодоступным в случае перехвата трафика. Базовая оценка CVSS, данная этим уязвимостям, указывает на их высокий риск.

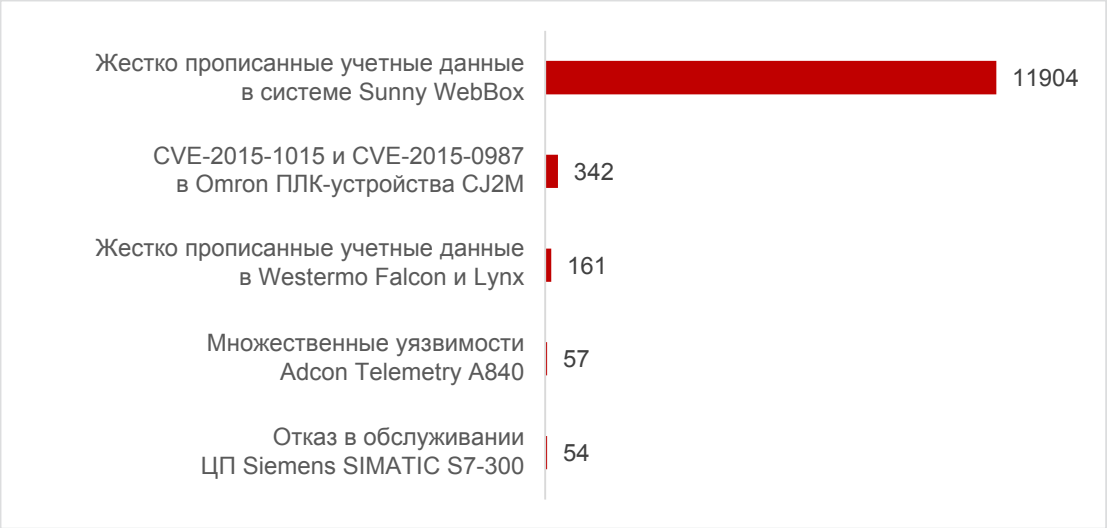

Рисунок 11. 5 главных уязвимостей в компонентах АСУ ТП

Объединив эти результаты со статистикой использования незащищенных протоколов (как описано ранее в разделе 3.4), мы смогли оценить **общее число уязвимых хостов с компонентами АСУ ТП — 172 982 хоста (92%)**. В большинстве случаев (87%) хосты содержали уязвимости со средним риском. Однако 7% уязвимых хостов имели критические уязвимости.

Рисунок 12. Статистика уязвимых хостов (по максимальному уровню критичности уязвимости на хост)

Что касается хостов, принадлежащих крупным организациям (см. ранее в разделе 3.5), 12 425 из них (90,7%) используют незащищенные протоколы. На 453 хостах (3,3%) были найдены другие типы уязвимостей. **Общее число уязвимых хостов АСУ ТП с внешним доступом, вероятно принадлежащих крупным компаниям, составляет 12 483 (91,1%)**.

453 хоста, включая хосты, принадлежащие энергетическим, транспортным, газовым и инженерно-производственным компаниям, содержат критические уязвимости. 96% уязвимых хостов содержат уязвимости со средним риском. Среди них хосты, принадлежащие энергетическим, нефтегазовым, транспортным, аэрокосмическим, аграрным, автомобильным компаниям, «умным» городам и производителям пищевых продуктов и напитков.

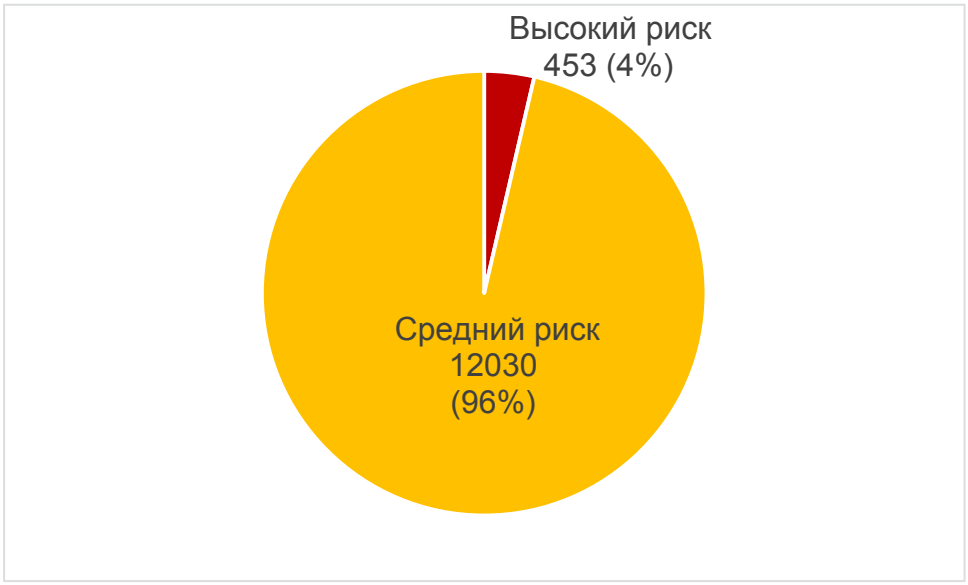

Рисунок 13. Статистика уязвимых корпоративных хостов
(по максимальному уровню критичности уязвимости на хост)

Мы также обнаружили внешние хосты с уязвимостями среднего риска в сетевых диапазонах, принадлежащие производителям решений АСУ ТП. Стоит отметить, что собственные решения производителей были не единственными доступными в их сетях.

Надо также сказать, что показанные выше результаты соответствуют нижней границе оценки: в действительности число компонентов АСУ ТП, доступных из внешних сетей, что сопряжено с высоким уровнем риска, может быть значительно выше. Кроме того, были оценены уровни рисков уязвимостей на основе базовых показателей Единой системы определения величины уязвимостей (Common Vulnerability Scoring System, CVSS) версий 2 и 3 в рамках общей оценки. Однако в средах АСУ ТП многое зависит от особенностей системы: порой даже некритические уязвимости могут оказать серьезное влияние на инфраструктуру, если удастся их задействовать. К примеру, успешно используя бреши в безопасности протокола Siemens S7 (со средним риском), злоумышленники могут выполнить несанкционированную перепрошивку ПЛК Siemens. Эта атака сходна с деятельностью червя Stuxnet: она может привести к полному отказу в обслуживании, помешав соответствующим технологическим процессам.

4 Заключение

Кибербезопасность АСУ ТП тесно связана с физической безопасностью населения. Однако подходы к их защите существенно различаются. Малые и средние компании, а также индивидуальные пользователи полностью полагаются на производителей во всем, что касается безопасности интернета вещей. Потребители не идут дальше базовых указаний в руководствах по эксплуатации устройств — в результате они получают готовые к работе и легкодоступные, но при этом уязвимые устройства. Крупные предприятия, напротив, понимают, что неправильная конфигурация среды, в которой работает АСУ ТП, связана с высоким уровнем риска. Но в результате владельцы систем АСУ ТП зачастую рассматривают их как своеобразные «черные ящики» и боятся вносить в их среду изменения, в том числе и направленные на повышение уровня кибербезопасности.

Выводы, сделанные на основе настоящего исследования, — дополнительное напоминание о том, что принцип Security through obscurity («безопасность через неясность») не может служить хорошей основой для эффективной защиты от современных атак и что информационная безопасность автоматизированных систем управления не должна приноситься в жертву их физической безопасности, тем более что в данном случае эти два вида безопасности неразрывно связаны между собой.

Решения для защиты крупного бизнеса: kaspersky.ru/enterprise