Безопасность промышленных систем в цифрах v2.1*

Глеб Грицай

Александр Тиморин

Юрий Гольцев

Роман Ильин

Сергей Гордейчик

Антон Карпин

Отдельная благодарность сообществу www.asutpforum.ru

МОСКВА
2012

СОДЕРЖАНИЕ

1. Введение 3

2. Выводы 4

3. Востребованность элементов систем АСУ ТП (SCADA) в России 5

4. Анализ уязвимостей систем АСУ ТП 9

4.1. Методика исследования 9

4.2. Динамика обнаружения уязвимостей 10

4.3. Количество уязвимостей АСУ ТП различных производителей 12

4.4. Уязвимости по типам программно-аппаратных компонентов АСУ ТП 14

4.5. Распределение уязвимостей по типам и возможным последствиям 15

4.6. Доля устраненных уязвимостей АСУ ТП 16

4.7. Доля оперативно устраненных уязвимостей АСУ ТП 18

4.8. Доступность сведений или ПО для проведения атаки 20

4.9. Количество эксплойтов 20

4.10. Степень риска обнаруженных уязвимостей 22

4.11. Неустраненные уязвимости АСУ ТП 24

5. Распространенность систем АСУ ТП в сети Интернет 25

5.1. Распространенность систем АСУ ТП 26

5.2. Типы систем АСУ ТП 30

5.3. Доли уязвимых и безопасных систем АСУ ТП 31

5.4. Типы уязвимостей 32

5.5. Доля уязвимых систем АСУ ТП в разных странах 33

5.6. Доля уязвимых систем АСУ ТП в разных регионах 35

6. Изменения 36

7. О компании 36

1. ВВЕДЕНИЕ

Современная цивилизация в значительной степени зависит от средств автоматизации производственных процессов АСУ ТП (ICS). Атомные и гидроэлектростанции, нефте- и газопроводы, национальные сети распределения электроэнергии, транспортные системы национального и мирового уровня функционируют на основе компьютерных технологий. И от защищенности систем управления подобными системами зависит не только прибыль компаний, но и национальная безопасность.

Широкий интерес к защищенности промышленных систем возник не так давно, после серии инцидентов со специализированными компьютерными вирусами, такими как Flame и Stuxnet. Тогда выяснилось, что спецслужбы иностранных государств, конкурирующие корпорации или кибертеррористы могут использовать в своих целях недостаточное внимание к информационной безопасности систем АСУ ТП и их компонентов (SCADA/PLC).

Еще одним стимулирующим фактором для российских специалистов в области ИБ является возникновение новых требований регулирующих органов и организаций, направленных на повышение безопасности промышленных систем.

При формировании системы защиты важными задачами являются построение модели угроз и модели потенциального злоумышленника. Для выбора адекватных мер безопасности необходимо понимать, какими возможностями обладает киберпреступник и какие векторы нападения он может использовать. Чтобы ответить на эти вопросы, эксперты Positive Technologies провели исследование безопасности систем АСУ ТП. Данный документ состоит из трех разделов, в которых представлены соответственно:

- анализ российского рынка компонентов АСУ ТП;
- статистика уязвимостей компонентов АСУ ТП;
- оценка распространенности компонентов АСУ ТП в сети Интернет.

Объектом исследования стали уязвимости, обнаруженные с 2005 г. по 1 октября 2012 г.

* По результатам обратной связи обновлена информация по Schneider Electric.

2. ВЫВОДЫ

1. История безопасности промышленных систем разделяется на два этапа: до появления Stuxnet и после. С 2010 года было обнаружено в 20 раз больше уязвимостей, чем за предыдущие пять лет.

АСУ ТП в цифрах:

С 2010 года в 20 раз выросло число обнаруженных уязвимостей.

Каждая пятая уязвимость устраняется дольше месяца.

50% уязвимостей позволяют хакеру запустить выполнение кода.

Для 35% уязвимостей есть эксплойты.

Более 40% интернет-доступных систем могут взломать хакеры-любители.

Треть доступных из интернета систем находятся в США.

Четверть уязвимостей связана с отсутствием необходимых обновлений безопасности.

Уязвимы 54% интернет-доступных систем в Европе и 39% в Северной Америке.

Уязвимы 50% опубликованных в глобальной сети систем из России.

2. В 2012 году продолжается стремительный рост числа уязвимостей. За десять месяцев было найдено больше недостатков безопасности, чем за весь предшествующий период.

3. Уязвимости обнаруживаются в первую очередь в самых популярных продуктах, и большинство производителей устраняют их достаточно оперативно. Однако при этом каждая пятая уязвимость не была закрыта в течение 30 дней с момента ее обнаружения.

4. Около 65% уязвимостей относятся к высокой и критической степени риска. Этот показатель значительно превышает аналогичный показатель в прочих IT-системах, что свидетельствует о низком уровне развития информационной безопасности систем АСУ ТП.

5. Эксплуатация каждой второй уязвимости позволяет злоумышленнику произвести выполнение произвольного кода на различных компонентах систем АСУ ТП.

6. Более 40% всех доступных из сети Интернет ICS-систем — уязвимы и могут быть взломаны низкоквалифицированным злоумышленником.

7. США и Европа лидируют по количеству доступных из сети Интернет компонентов АСУ ТП и демонстрируют наиболее легкомысленное отношение к их защищенности по сравнению со всеми прочими регионами.

8. Более трети недостатков безопасности присутствующих в сети Интернет компонентов АСУ ТП вызвана ошибками конфигурации, включая наличие стандартных инженерных паролей в исходном виде.

9. Четвертая часть уязвимостей интернет-доступных компонентов АСУ ТП связана с отсутствием необходимых обновлений безопасности.

3. ВОСТРЕБОВАННОСТЬ КОМПОНЕНТОВ СИСТЕМ АСУ ТП (SCADA) В РОССИИ

Для того чтобы понимать, насколько опасны те или иные уязвимости автоматизированных систем управления, необходимо оценить степень локального проникновения различных производителей на российский рынок.

Основой для анализа послужила статистика базы вакансий портала hh.ru. Мы получили представление о степени востребованности специалистов, обладающих опытом работы с той или иной системой, технологией, протоколом или программным продуктом. На основании этих данных можно приблизительно оценить доли различных производителей на рынке программных и аппаратных составляющих систем АСУ ТП[1].

Согласно полученным данным, наиболее востребованными являются специалисты, имеющие навыки работы с решениями компании Siemens. Из шести самых распространенных продуктов четыре относятся к семейству Siemens SIMATIC:

- STEP 7 — разработка систем автоматизации на основе PLC;
- WinCC и WinCC Flexible — создание человеко-машинного интерфейса;
- PCS 7 — построение комплексных систем автоматизации.

В пятерку лидеров также входят InTouch компании Invensys Wonderware и пакет ПО Genesis от Iconics.

[1] В статистику вошли только продукты и технологии, имеющие известные к настоящему моменту уязвимости. На российском рынке достаточно распространены решения АСУ ТП местных производителей. Однако, поскольку информация о проблемах безопасности этих систем недоступна, они не были включены в отчет.

Таблица 1. Востребованность специалистов АСУ ТП

Программные продукты	Количество упоминаний
STEP7 (Siemens)	28
WinCC (Siemens)	23
InTouch (Invensys Wonderware)	17
PCS7 (Siemens)	10
Genesis (Iconics)	7
WinCC Flexible (Siemens)	5
iFIX (Intellution)	5
Indusoft Web Studio (InduSoft)	4
Trace Mode (AdAstrA)	3
Rsview (Rockwell automation)	2
SPPA-T3000 (Siemens)	2
DeltaV (Emerson)	2
Citect (Schneider Electric)	2
Решения Fraunc-GE	2
GraphWorX (Iconics)	1
SCADA Infinity Suite (ЭлеСи)	1
PACiS (AREVA)	1
Решения General Electric	1
Решения Advantech	1
CoDeSys (3S-Smart Software Solutions)	1
ISaGRAF (ICS Triplex ISaGRAF)	1
CX-Supervisor (Omron)	1
ProTool (Siemens)	1
Решения ProLeit	1
Решения Vipa	1
Решения Delta	1
Решения Mitsubishi	1
Решения OSIsoft	1
MicroSCADA	1

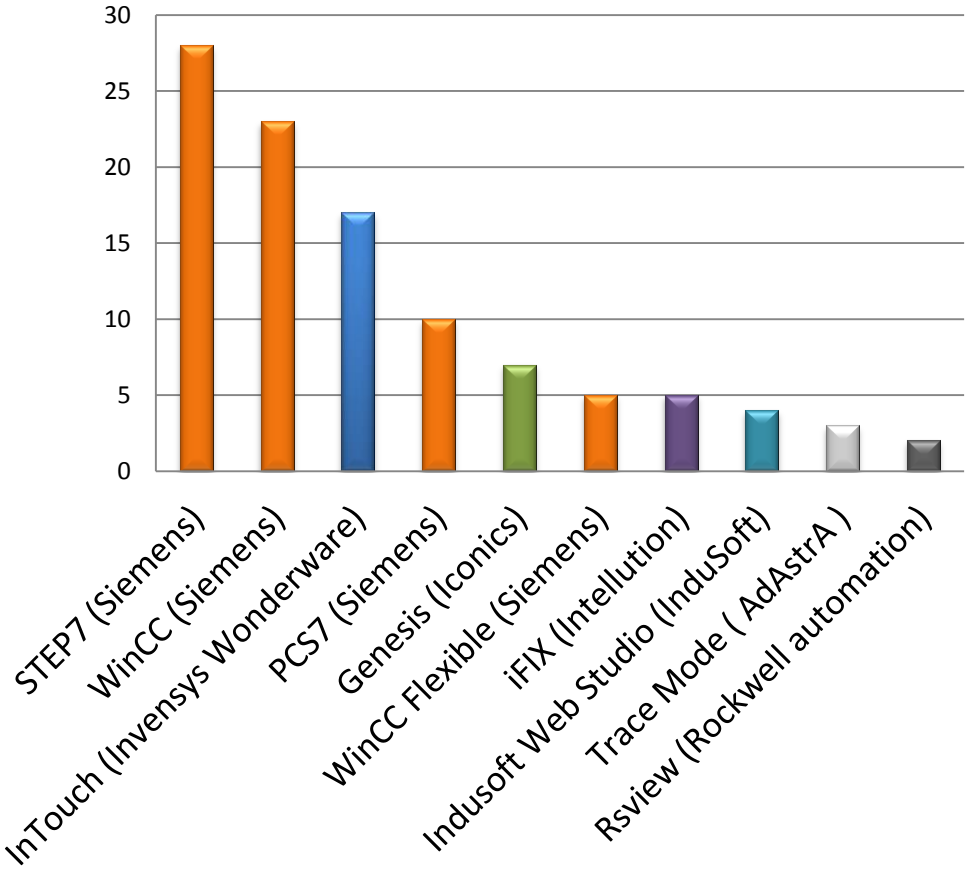

Рис. 1. Востребованность специалистов АСУ ТП

Если рассматривать технологии передачи данных, то наиболее востребованными являются специалисты со знанием Modbus (RTU и TCP/IP) и Profibus/Profinet, далее следует OPC.

Таблица 2. Востребованность специалистов по сетевым технологиям

Технологии и протоколы	**Количество упоминаний**
Modbus (TCP + RTU)	17
Profibus/Profinet	17
OPC	13
DNP3	2
ICCP	1
Другие	2

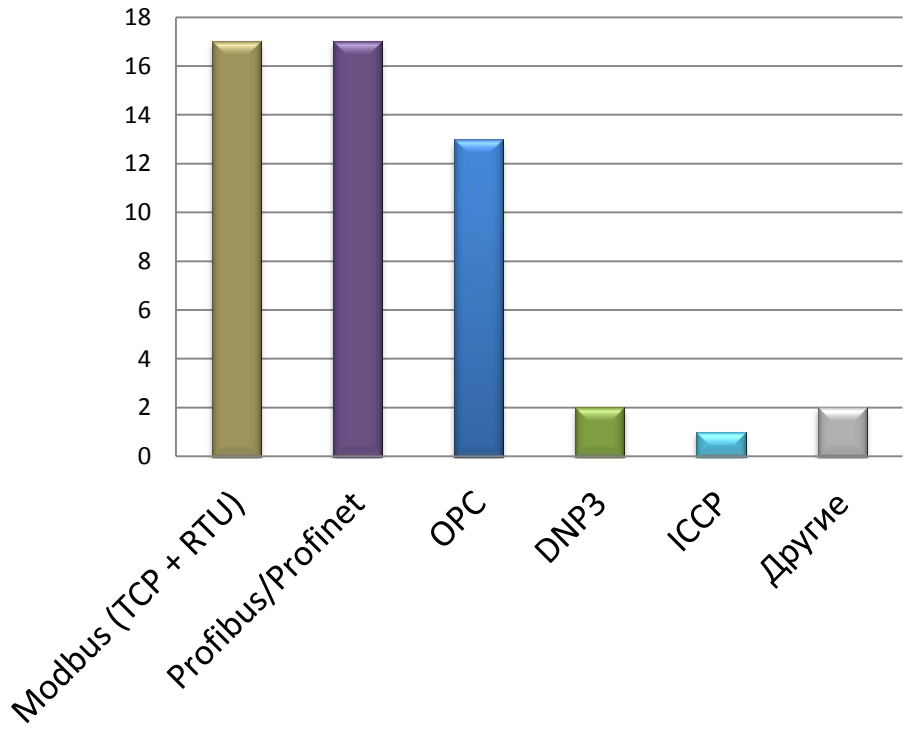

Рис. 2. Востребованность специалистов по сетевым технологиям

Среди всех используемых операционных систем АСУ ТП с большим отрывом лидирует Microsoft Windows, опыт работы с которой требуется в большинстве объявлений о вакансиях в этой сфере. О необходимости знать QNX и FreeRTOS свидетельствует лишь незначительное количество объявлений.

В сегменте программируемых логических контроллеров чаще всего требуются специалисты по решениям Siemens (примерно 31%). Далее следуют продукты Schneider Electric (11%), ABB (9%), Rockwell Automation (7%) и Emerson (5%).

Таблица 3. Востребованность специалистов по ПЛК

Производители ПЛК (PLC)	**Доля, %**
Siemens	30,6
Schneider Electric	10,8
ABB	8,6
Rockwell Automation	6,8
Emerson	5
GE	4,5
Honeywell	3,6

Yokogava	3,2
Omron	3,2
Другие	23,9

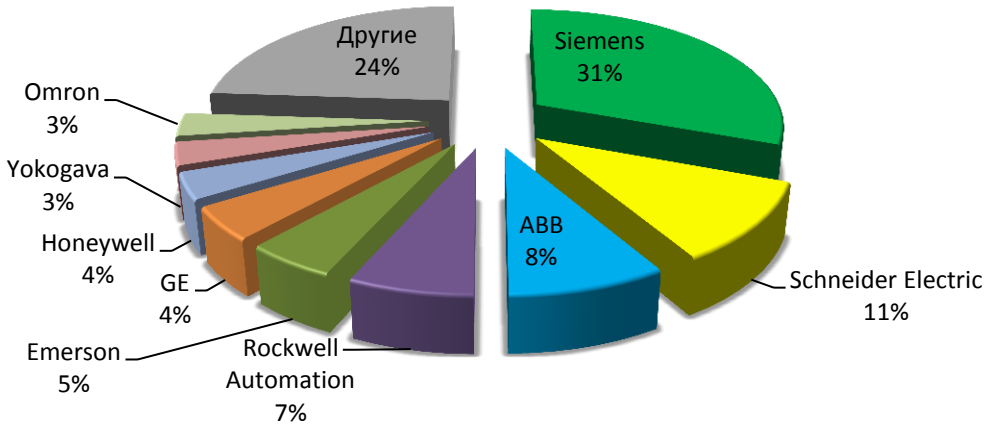

Рис. 4. Востребованность специалистов по ПЛК

4. АНАЛИЗ УЯЗВИМОСТЕЙ КОМПОНЕНТОВ АСУ ТП

4.1. Методика исследования

В качестве основы для исследования была использована информация из различных источников, таких как базы знаний уязвимостей (vulnerability databases) и уведомления производителей, сборники эксплойтов (exploit packs), доклады научных конференций, публикации на специализированных сайтах и в блогах. Необходимость анализа столь широкого спектра источников связана с тем, что взаимодействие между профессиональным сообществом исследователей в области ИБ и производителями АСУ ТП в настоящее время только выстраивается, и многие уязвимости публикуются без согласования с разработчиками.

Основные источники, используемые в исследовании

Базы знаний по уязвимостям:

- ICS-CERT,
- NVD,
- CVE,
- Bugtraq,
- OSVDB,
- Mitre Oval Repositories,
- exploit-db,
- Siemens Product CERT.

Сборники эксплойтов:

- SAINTexploit,
- Metasploit Framework,
- Immunity Canvas,
  - Agora Pack,
  - Agora SCADA+,
  - D2 Exploit Pack,
  - White Phosphorus exploit pack,
  - VulnDisco Exploit Pack.

Для каждой выявленной уязвимости проводился поиск общедоступных методов использования (эксплойтов) и давалась экспертная оценка рисков, связанных с последствиями ее использования.

4.2. Динамика обнаружения уязвимостей

В период с 2005 г. до начала 2010 г. специалисты по информационной безопасности обнаружили всего лишь 9 уязвимостей. После появления компьютерного червя Stuxnet произошел резкий скачок интереса как со стороны исследователей ИБ, так и со стороны хакеров. В итоге в 2011 г. в компонентах АСУ ТП было обнаружено 64 уязвимости. И только за первые восемь месяцев 2012 года стало известно о 98 новых уязвимостей: это больше, чем за все предыдущие годы, начиная с 2005 г.

Иногда уязвимости ICS/SCADA-систем проходят достаточно извилистый путь от обнаружения до устранения. Как было выяснено в ходе расследования инцидента, связанного с червем Stuxnet, одна из использованных вирусом уязвимостей — стандартный пароль для Microsoft SQL Server — была известна уже давно. Впервые о ней упоминали на форумах поддержки в мае 2005 года, а в открытом доступе пароли были опубликованы в апреле 2008 года. Устранена проблема была лишь после атаки — в 2010 году.

Таблица 5. Количество обнаруженных уязвимостей

Годы	Количество уязвимостей
2005	1
2007	3
2008	5
2010	11
2011	64
2012	98

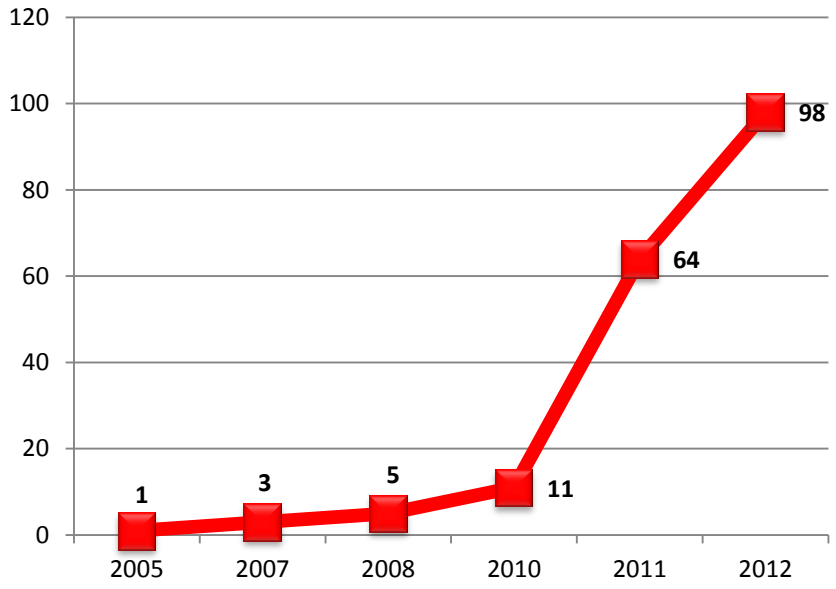

Рис. 6. Динамика количества уязвимостей

4.3. Количество уязвимостей в системах различных производителей

Наибольшее количество уязвимостей (42) за отчетный период было обнаружено в компонентах АСУ ТП производства компании Siemens. На втором месте — системы Schneider Electric (30). На третьем — Broadwin/Advantech (22 уязвимости).

Таблица 7. Количество уязвимостей компонентов АСУ ТП различных производителей

Производитель	Количество уязвимостей
Automated Solutions	2
Schweitzer Engineering Laboratories	2
RuggedCom	2
Lantronix	3
Progea	3
ABB	3
Sielco Sistemi	3
Iconics	5
Measuresoft	6
Ecava	5

Emerson	6
Rockwell Automation	9
WellinTech	9
General Electric	15
Invensys Wonderware	15
Advantech/Broadwin	22
Schneider Electric	30
Siemens	42

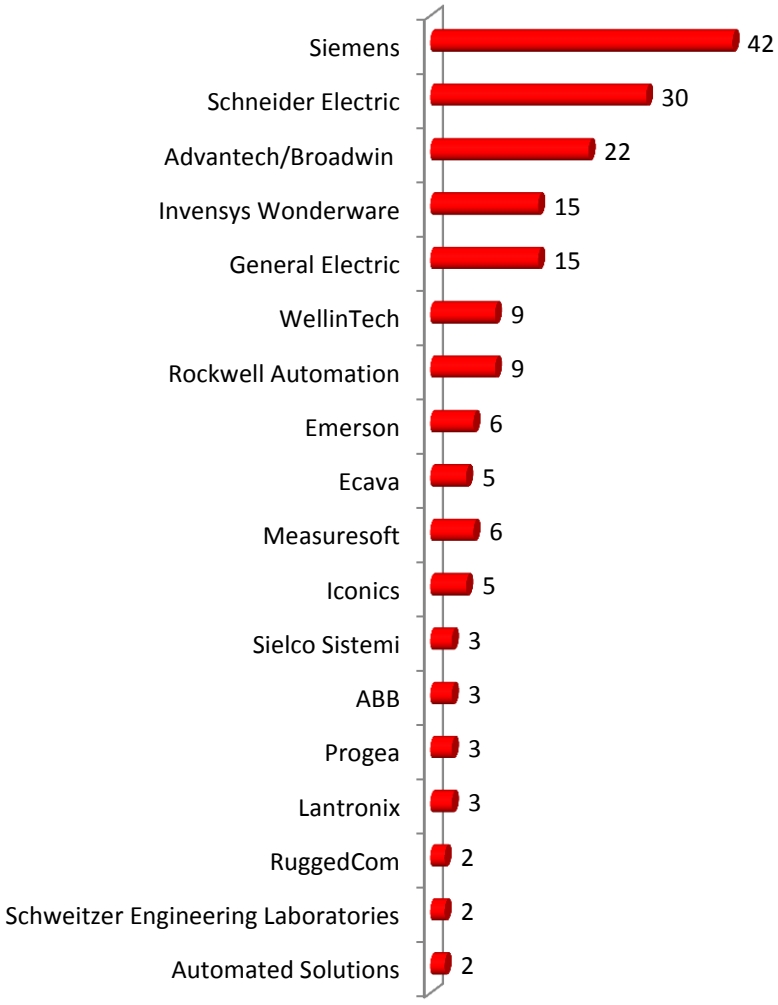

Рис. 8. Количество уязвимостей компонентов АСУ ТП различных производителей

Как в любых IT-системах, в случае с АСУ ТП наибольшее количество уязвимостей обнаруживается в самых распространенных решениях. Кроме того, ряд производителей перешли от реактивного подхода к проактивному, и энергично занялись поиском и устранением уязвимостей в своих продуктах. К примеру, компания Siemens сформировала специализированное подразделение Siemens ProductCERT (http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm), основной задачей которого является обнаружение и устранение проблем безопасности в продуктах компании. Найденные этой командой уязвимости также включаются в общую статистику, что приводит к росту абсолютных значений обнаруженных и устраненных проблем.

4.4. Уязвимости по типам программно-аппаратных компонентов АСУ ТП

Наибольший интерес для злоумышленников могут представлять такие составляющие АСУ ТП, как системы SCADA и человеко-машинного интерфейса (HMI), в которых обнаружено 87 и 49 уязвимостей соответственно. В программируемых логических контроллерах различных производителей за отчетный период нашли 20 уязвимостей. Уязвимости средств разработки, как правило не являются чем-то специфическим и совпадают с уязвимостями компонентами SCADA/HMI,входящих в средства разработки.

Таблица 6. Количество уязвимостей в различных типах компонентов АСУ ТП

Тип системы	Количество уязвимостей
SCADA	87
HMI	49
PLC	20
Hardware	11
Software	7
Interface/Protocol	1

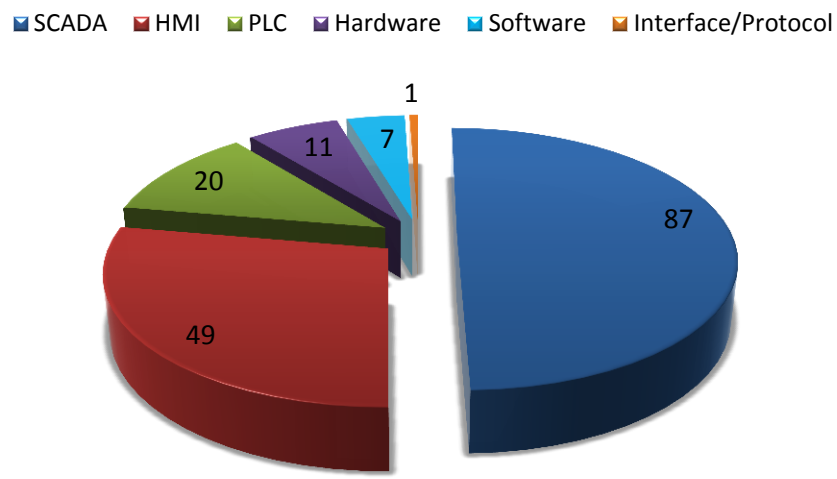

Рис. 6. Количество уязвимостей в различных типах компонентов АСУ ТП

4.5. Распределение уязвимостей по типам и возможным последствиям

Почти треть уязвимостей (36%) связаны с переполнением буфера (Buffer Overflow) — явлением, возникающим, когда компьютерная программа записывает данные за пределами выделенного в памяти буфера. Подобный недостаток защищенности позволяет злоумышленнику не только вызвать аварийное завершение или «зависание» программы (что ведет к отказу в обслуживании), но и выполнять в целевой системе произвольный код. Если же сложить все типы уязвимостей, эксплуатация которых позволяет хакеру запустить выполнение кода (Buffer Overflow, Remote Code Execution), то получится около 50% всех уязвимостей (крайне высокая цифра!). Стоит отметить также большое количество проблем с аутентификацией и управлением ключами (Authentication, Key Management; почти 23%).

Рост количества обнаруженных уязвимостей в системах АСУ ТП в последние годы обусловлен также и тем, что к процессу подключились организованные команды этических хакеров. Экспертами исследовательского центра Positive Research в 2012 году было обнаружено более 50 уязвимостей в различных продуктах, большая часть которых в настоящее время уже устранена производителями. Значительную работу по координации устранения проводит также организация ICS CERT.

Таблица 7. Распределение уязвимостей АСУ ТП по типу

Тип уязвимости	Доля уязвимости, %
Buffer Overflow	36
Remote Code Execution	13,14
Web (client-side)	9,14
Web (server-side)	10,86
Local Privilege Escalation	2,29
DoS/Data Integrity	5,71
Authentication / Key Management	22,86

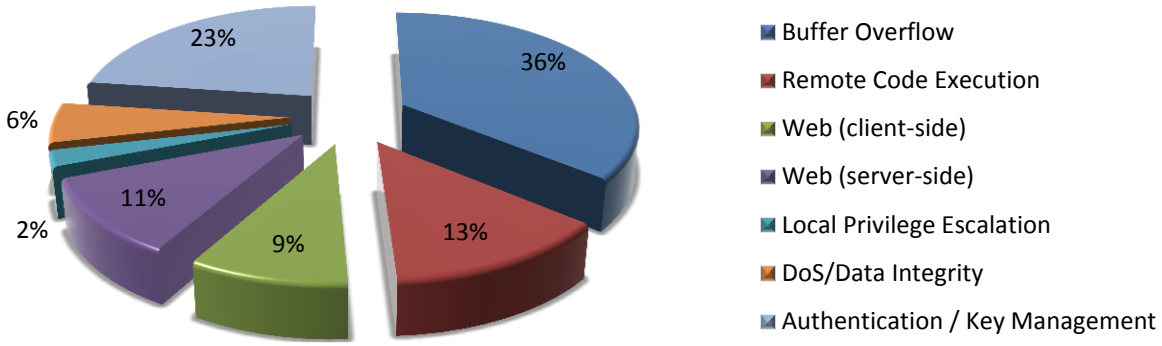

Рис. 7. Распределение уязвимостей компонентов АСУ ТП по типу

4.6. Доля устраненных уязвимостей компонентов АСУ ТП

Наглядное представление о том, насколько серьезно различные производители АСУ ТП относятся к проблемам информационной безопасности, дает демонстрация доли устраненных уязвимостей. Например, компания Siemens устранила и выпустила обновления для 88% уязвимостей, тогда как ABB ликвидировала только две трети (67%) недостатков защищенности.

Таблица 8. Доля устраненных уязвимостей АСУ ТП

Производители	Устраненные, %
Advantech/Broadwin	91
WellinTech	89

Siemens	88
General Electric	80
Rockwell Automation	78
ABB	67
Schneider Electric	56
Lantronix	—
Schweitzer Engineering Laboratories	—
Всего	**84**

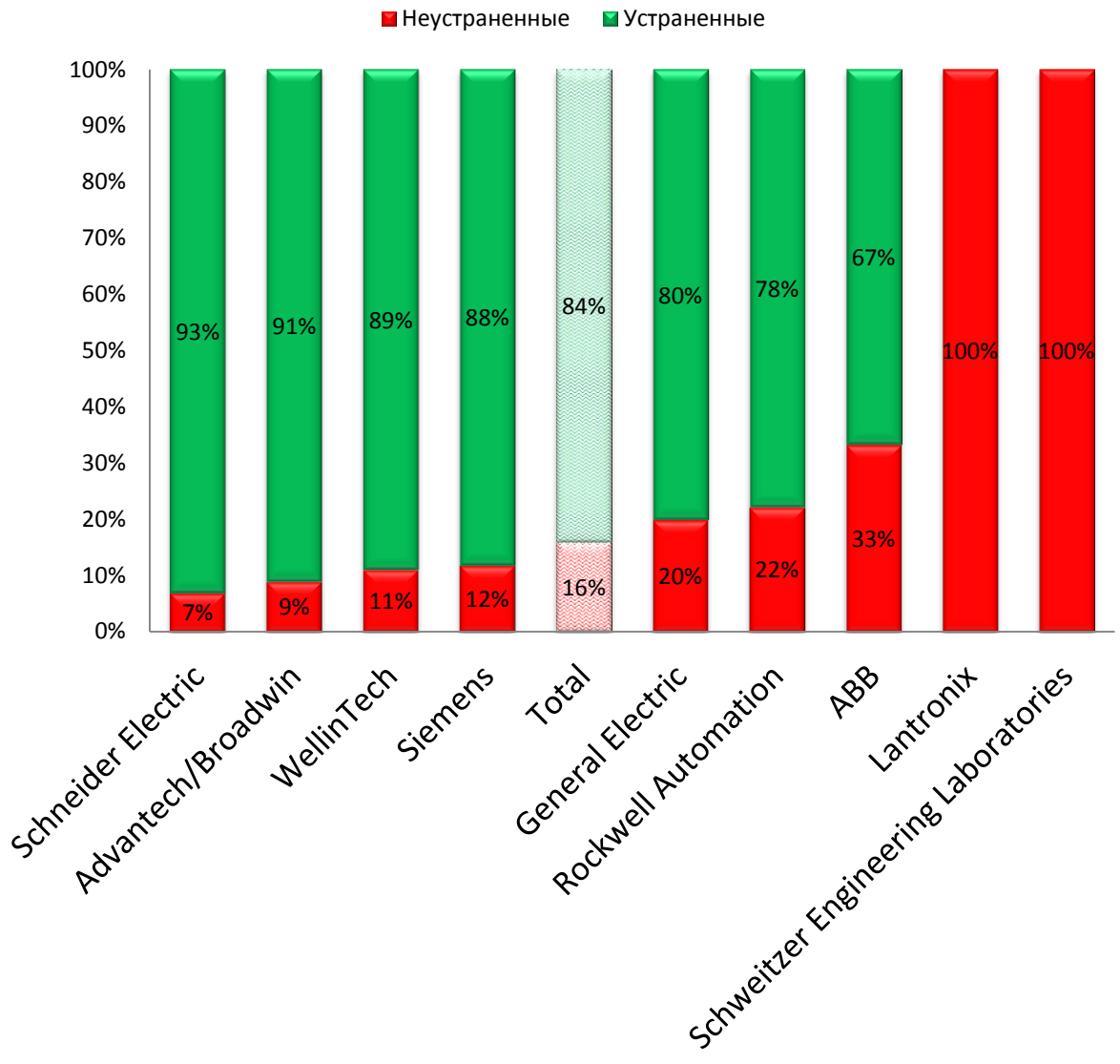

Рис. 8. Доля устраненных уязвимостей компонентов АСУ ТП

4.7. Доля оперативно устраненных уязвимостей компонентов АСУ ТП

Большинство недостатков безопасности (около 81%) были достаточно оперативно ликвидированы производителями компонентов АСУ ТП — еще до того, как сведения о них становились широко известны, или в течение 30 дней после нескоординированного разглашения информации. Однако примерно каждая пятая уязвимость «закрывалась» с серьезной задержкой, а в некоторых случаях так и не была устранена.

В августе 2010 года было опубликовано уведомление US-CERT VU#362332, в котором сообщалось об опасной уязвимости в системе реального времени VxWorks, используемой в промышленности. По утверждению исследователя HD Moore, он обнаружил более 250 000 уязвимых систем, доступных из сети Интернет.

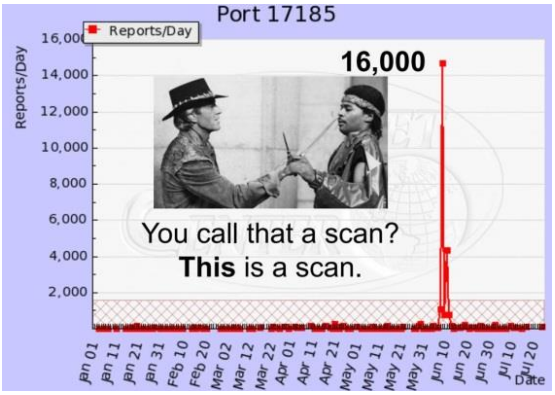

Рис. 9. Доля оперативно устраненных уязвимостей компонентов АСУ ТП

4.8. Доступность сведений или ПО для проведения атаки

Наличие в открытом доступе информации или готового средства для эксплуатации уязвимости значительно повышает вероятность успешной реализации атаки. В настоящий момент для 35% всех представленных уязвимостей АСУ ТП выпущены эксплойты, которые свободно распространяются в виде отдельных утилит, входят в состав программных пакетов для проведения тестов на проникновение либо описаны в уведомлениях об уязвимости.

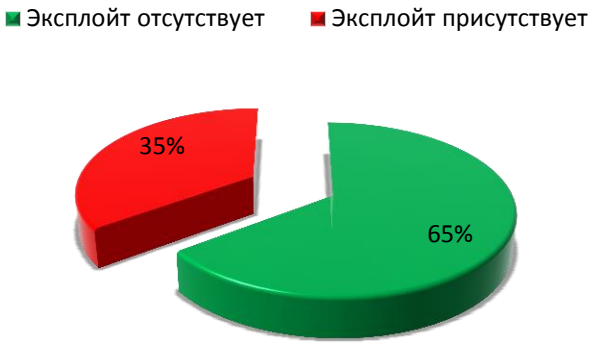

Рис. 9. Доля уязвимостей, для которых есть эксплойты

Следует отметить, что 35% — достаточно высокое значение для количества доступных эксплойтов: оно в разы превышает аналогичный показатель для IT-систем вообще.

4.9. Количество эксплойтов

Как правило, количество обнаруженных уязвимостей коррелирует с количеством опубликованных эксплойтов. В период с 2011 г. по сентябрь 2012 г. было опубликовано 50 эксплойтов: это в шесть раз больше, чем за период с 2005 по 2010 г.

Таблица 9. Динамика возникновения эксплойтов

Годы	Число эксплойтов
2008	2
2010	6
2011	30
2012	20

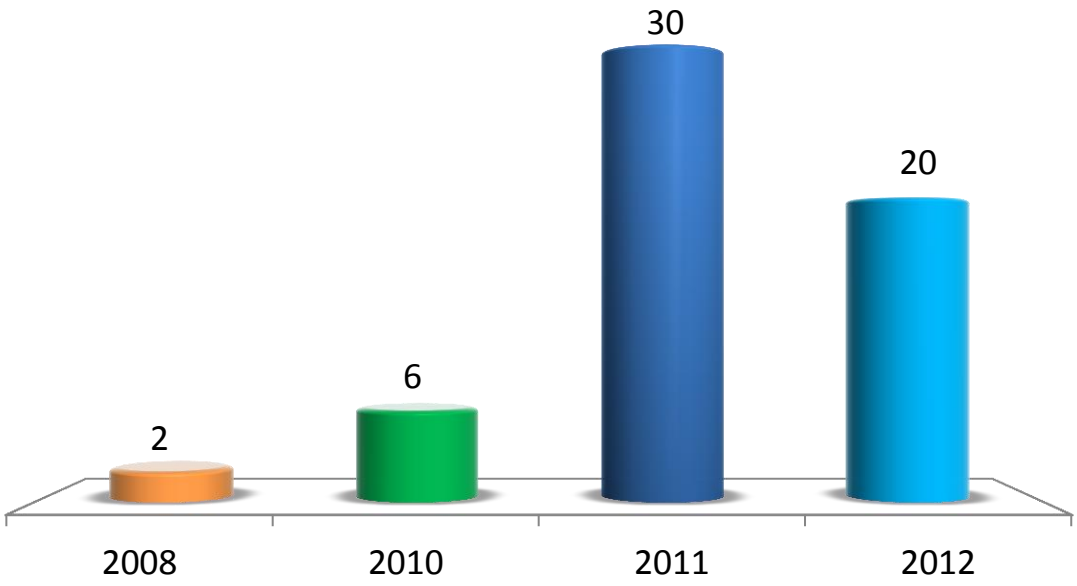

Рисунок 10. Динамика возникновения эксплойтов

Относительно небольшое количество эксплойтов, появившихся в 2012 г., может быть связано с двумя факторами:

- с упорядочиванием взаимоотношений между производителями АСУ ТП и исследователями, переходом к политике ответственного разглашения[2];
- с традиционной задержкой между публикацией информации об уязвимости и выходом эксплойтов (разработка средства для эксплуатации уязвимости требует определенных затрат).

[2] http://www.securitylab.ru/analytics/241826.php

4.10. Степень риска обнаруженных уязвимостей

Достаточно большое количество уязвимостей — почти 65% — относятся к высокой или критической степени риска[3].

Рис. 11. Распределение уязвимостей по степени риска

Наибольшую опасность представляют критические уязвимости (имеющие опубликованный эксплойт).

[3] Уязвимости высокой степени риска имеют значение CVSS v2 Base Score > 6,5. Уязвимостями критической степени риска являются уязвимости высокой степени риска, для которых имеется эксплойт.

Таблица 12. Уязвимости АСУ ТП по степени риска

	Критическая, %	Высокая, %	Средняя, %	Низкая, %
SEL	—	50	50	—
Lantronix	—	33	33	33
Emerson	—	40	40	20
Invensys Wonderware	—	47	40	13
Rockwell Automation	11	56	33	—
Siemens	14	42	31	14
General Electric	20	67	7	7
Advantech/Broadwin	23	45	23	9
ABB	33	67	—	—
Ecava	33	17	33	17
Schneider Electric	40	20	27	13
Measuresoft	40	40	20	—
Iconics	40	40	—	20
Automated Solutions	50	50	—	—
WellinTech	56	33	11	—
Progea	67	33	—	—
Sielco Sistemi	67	33	—	—
RuggedCom	100	—	—	—

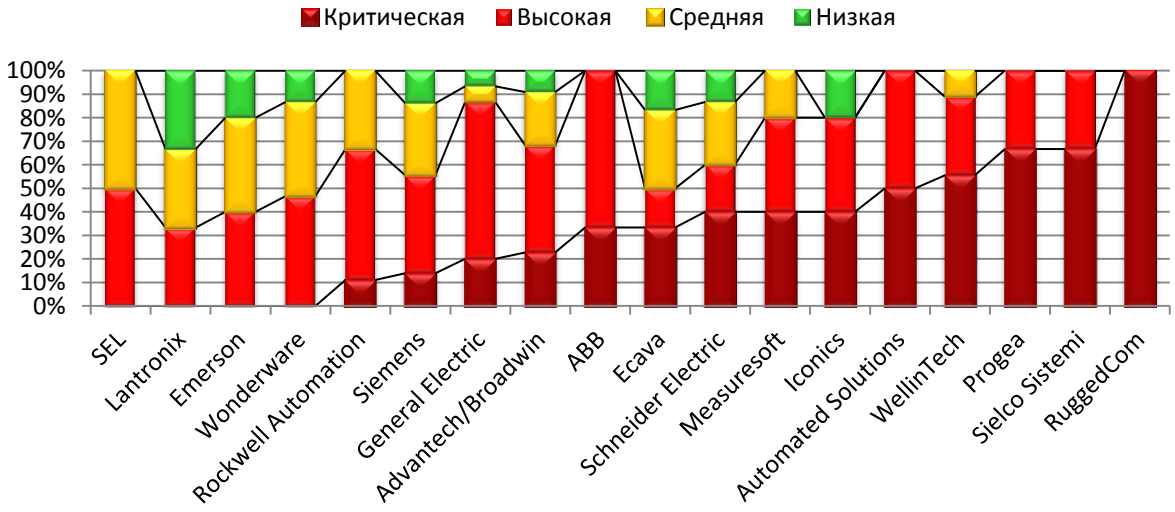

Рис. 13. Уязвимости компонентов АСУ ТП по степени риска

Отсутствие известного способа реализации атаки снижает вероятность нападения на компоненты АСУ ТП компаний SEL, Lantronix, Emerson и Invensys, но совершенно ее не исключает. Кибератака на промышленный объект, как правило, представляет собой многоходовую операцию с привлечением опытных специалистов, не нуждающихся в «эксплойт-паках» и других инструментах, рассчитанных в основном на массовую аудиторию хакеров.

В твиттере @ntisec постоянно публикуется информация о системах АСУ ТП, доступных из Интернет. Однажды на Pastebin.com было опубликовано более 2000 IP-адресов SCADA-систем, расположенных в различных регионах мира.

4.11. Неустраненные уязвимости компонентов АСУ ТП

Уязвимости, для которых уже существуют средства реализации атаки, но нет метода противодействия, представляют наибольший риск. Наличие эксплойта вкупе с отсутствием исправления повышает риск проникновения систему, поскольку для его осуществления злоумышленнику не требуются глубокие знания и длительная подготовка операции; атака может быть совершена из хулиганских побуждений. Наиболее удручающая ситуация складывается в отношении компонентов АСУ ТП компании General Electric: обнаружено три уязвимости. На втором месте — компания Schneider Electric (2 уязвимости), третье и четвертое разделили Advantech/Broadwin и Rockwell Automation: по одной открытой уязвимости.

Таблица 14. Количество неустраненных уязвимостей компонентов АСУ ТП, для которых существуют эксплойты

Производитель	Число уязвимостей
Advantech/Broadwin	1
Rockwell Automation	1
Schneider Electric	2
General Electric	3

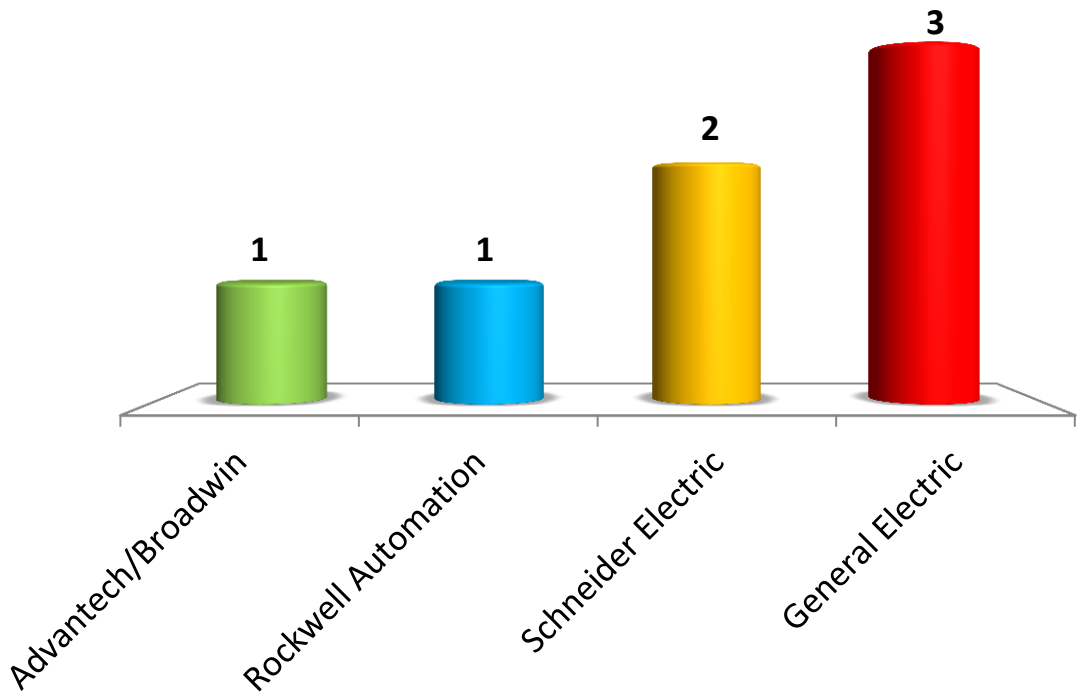

Рис. 15. Количество неустраненных уязвимостей компонентов АСУ ТП, для которых существуют эксплойты

5. РАСПРОСТРАНЕННОСТЬ КОМПОНЕНТОВ АСУ ТП В СЕТИ ИНТЕРНЕТ

Для того чтобы понять, в какой мере описанные выше уязвимости могут быть использованы злоумышленником, было проведено обследование сети Интернет на предмет наличия уязвимых компонентов АСУ ТП. Поиск и проверка версий систем осуществлялась методами пассивного анализа с использованием поисковых машин (Google, Yahoo, Bing) и специализированных баз знаний, таких как ShodanHQ, Every Routable IP Project. Полученная информация была проанализирована с точки зрения

наличия уязвимостей, связанных с управлением конфигурацией, и уязвимостей, связанных с установкой обновлений.

К сожалению, использование пассивной методики не позволяет достоверно идентифицировать все выявленные уязвимости, поэтому большую часть информации в данном разделе нужно расценивать в качестве позитивного сценария: при детальном анализе количество обнаруженных уязвимостей неминуемо возрастет.

5.1. Распространенность компонентов АСУ ТП

Почти треть компонентов АСУ ТП, к элементам которых есть доступ из сети Интернет, расположены в США (31,3%). На втором месте с большим отрывом находится Италия (6,8%), замыкает тройку Южная Корея (6,2%). Россия занимает 12 позицию с 2,3%, а в КНР находятся только 1,1% всех видимых из глобальной сети систем АСУ ТП.

Таблица 12. Распространение компонентов АСУ ТП по странам

Страна	Доля компонентов, %
США	31,3
Италия	6,8
Южная Корея	6,2
Канада	5,6
Индия	4,8
Чехия	3,9
Франция	3,9
Польша	3,1
Германия	2,8
Тайвань	2,8
Нидерланды	2,5
Россия	2,3
Испания	2,3
Австрия	1,7
Финляндия	1,7
Швеция	1,7
Швейцария	1,7
Великобритания	1,4
Китай	1,1
Прочие страны	12,4

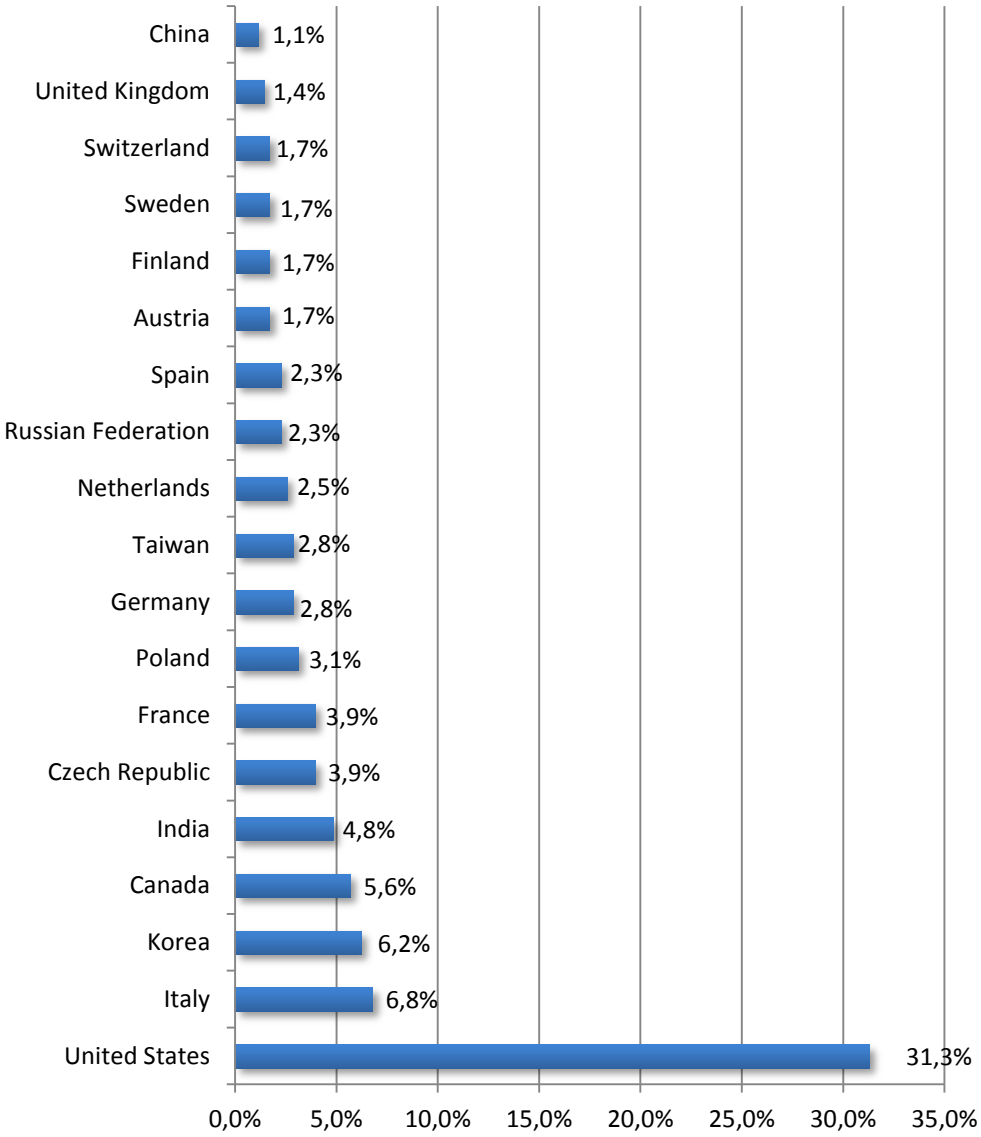

Рис. 12. Распространение компонентов АСУ ТП по странам

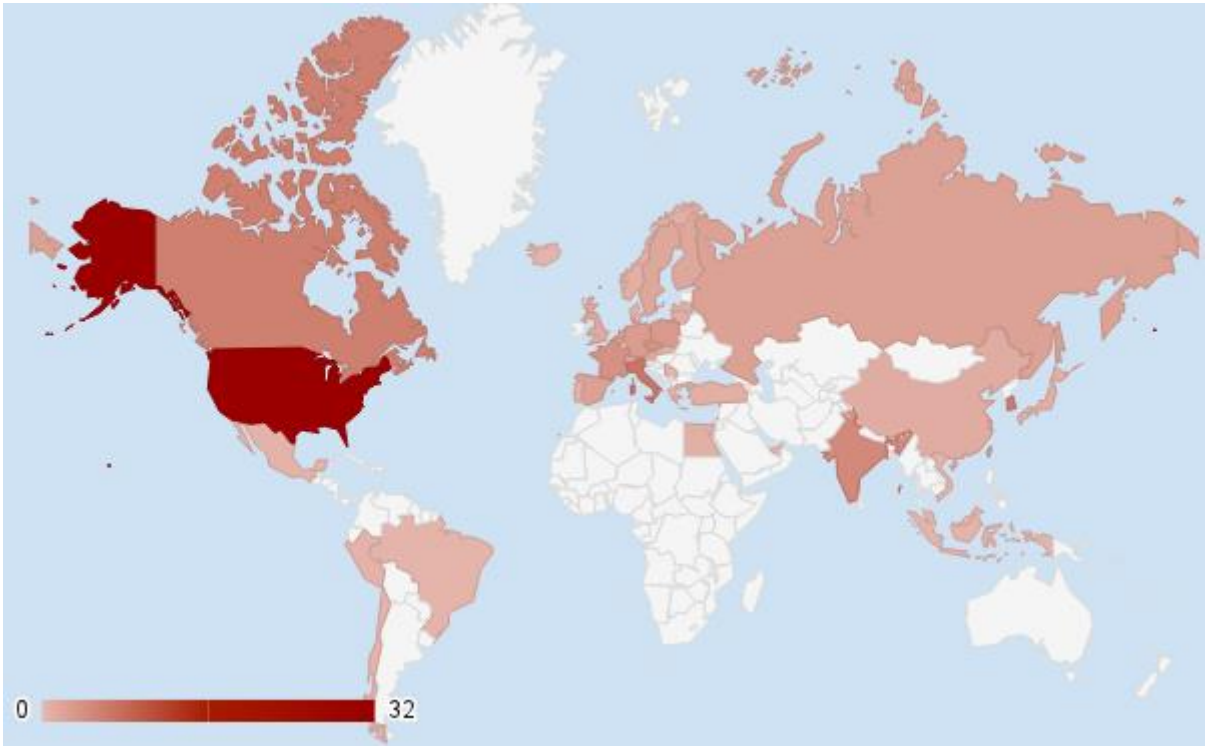

Рис 13. Распространение компонентов АСУ ТП по странам

В европейском регионе, несмотря на скромные цифры по отдельным странам, наблюдается наибольшее присутствие интернет-доступных компонентов АСУ ТП (41,41%). Старому Свету немного уступает Северная Америка (37,46%), на третьем месте — Азиатский регион (12,39%).

Таблица 13. Распространение компонентов АСУ ТП по регионам

Регион	Доля компонентов, %
Europe	41,41
North America	37,46
Asia	12,39
India	4,79
MEA[4]	2,82
South America	1,13

[4] Middle East and Africa

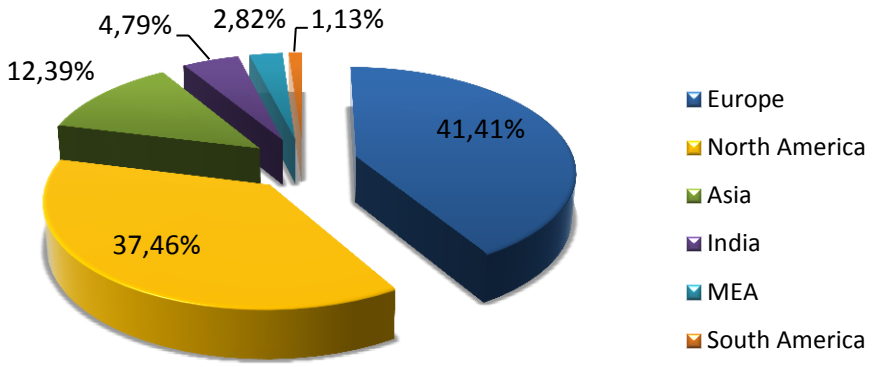

Рис. 14. Распространение компонентов АСУ ТП по регионам

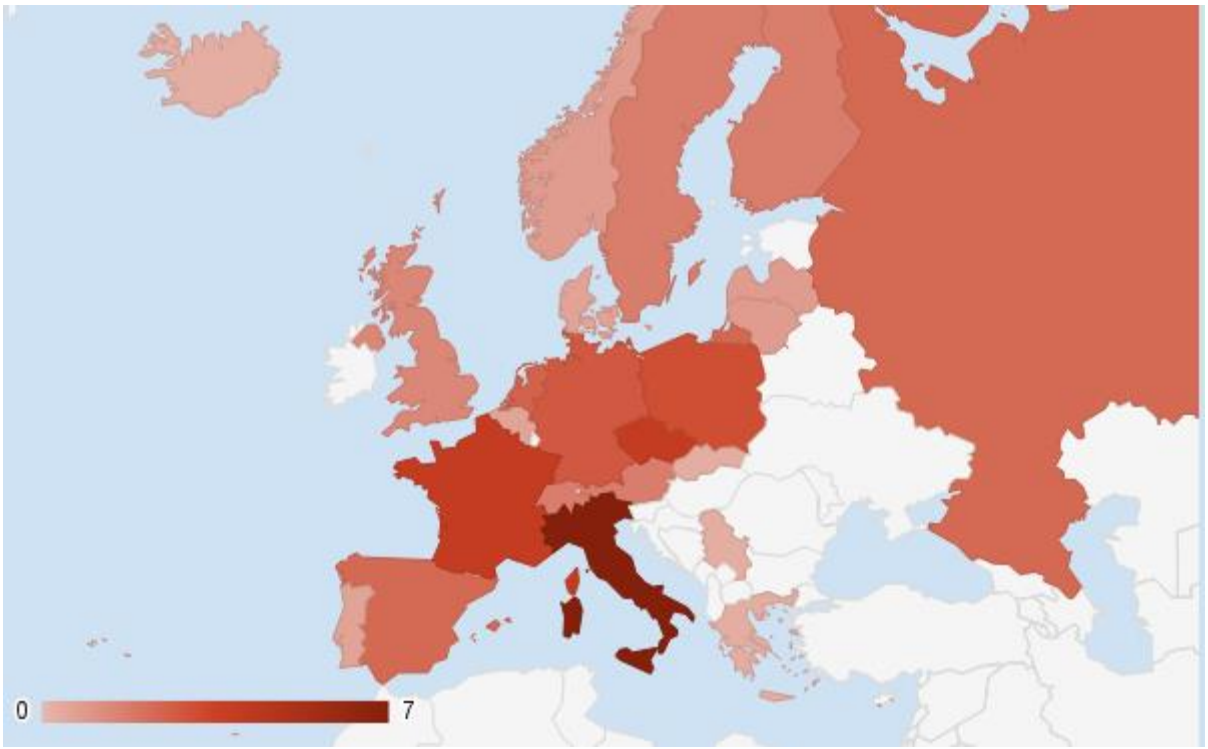

Рис. 15. Распространение компонентов АСУ ТП в Европе

Результаты ожидаемы, поскольку количество доступных систем напрямую зависит от степени автоматизации инфраструктуры.

5.2. Типы компонентов АСУ ТП

Чаще всего в глобальной сети присутствуют различные компоненты SCADA-систем, включая сетевые HMI. На их долю приходится 70% всех обнаруженных объектов. Еще 27% доступных компонентов АСУ ТП — это программируемые логические контроллеры. В 3% случаев были обнаружены различные сетевые устройства, используемые в сетях АСУ ТП (именуемые в таблице как Hardware).

Таблица 14. Компоненты АСУ ТП

Тип	Мировая доля, %
Hardware	3
HMI	27
PLC	27
SCADA	12
SCADA/HMI	31

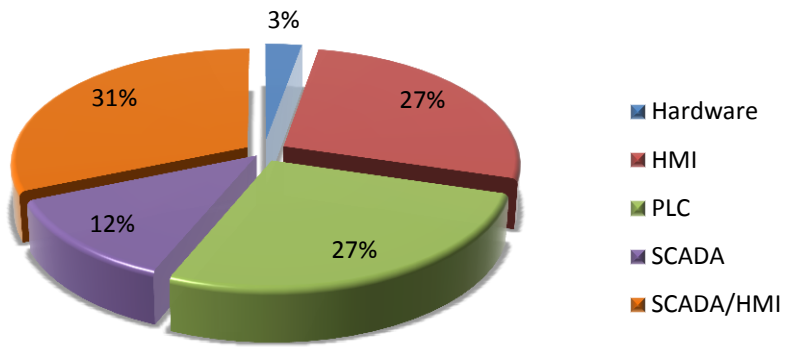

Рис. 16. Компоненты АСУ ТП

5.3. Доли уязвимых и безопасных компонентов АСУ ТП

Как минимум 42% доступных через Интернет компонентов АСУ ТП содержат уязвимости, которыми может без труда воспользоваться злоумышленник. Примерно такое же количество компонентов (41%) находятся в зоне риска, однако, как было сказано выше, применение пассивной методики обследования не позволяет достоверно идентифицировать все выявленные в них недостатки защищенности. Таким образом, в этой неизвестной зоне может скрываться значительная доля уязвимых систем. Доля систем, безопасность которых была достоверно подтверждена в ходе исследования, составляет всего лишь 17%.

Таблица 15. Доля уязвимых и безопасных компонентов АСУ ТП

Статус систем	Мировая доля, %
Безопасные	17
Статус неизвестен	41
Уязвимые	42

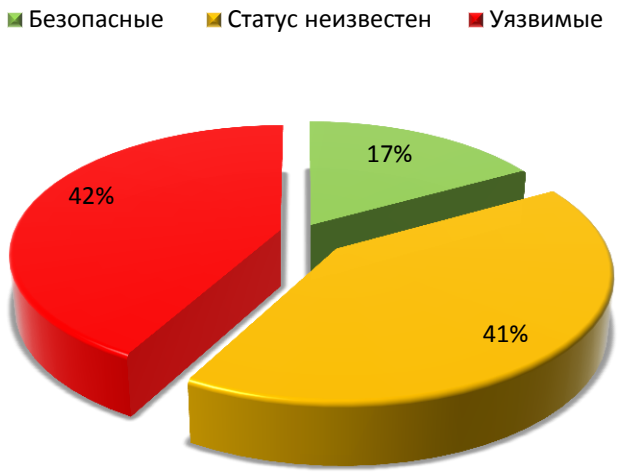

Рис. 17. Доля уязвимых и безопасных компонентов АСУ ТП

5.4. Типы уязвимостей

Недостатки безопасности, связанные с ошибками конфигурации, которые являются самыми распространенными, были выявлены в 36% всех случаев. Сюда относятся некорректная парольная политика (включая наличие в исходном виде стандартных инженерных паролей), доступ к критической информации, ошибочное разграничение полномочий пользователей и т. п. Четверть уязвимостей (25,35%) связана с отсутствием необходимых обновлений безопасности.

Таблица 16. Типы уязвимостей

Тип уязвимости	Мировая доля, %
Комбинированный	41,97
Ошибки конфигурации	36,06
Управление обновлениями	25,35

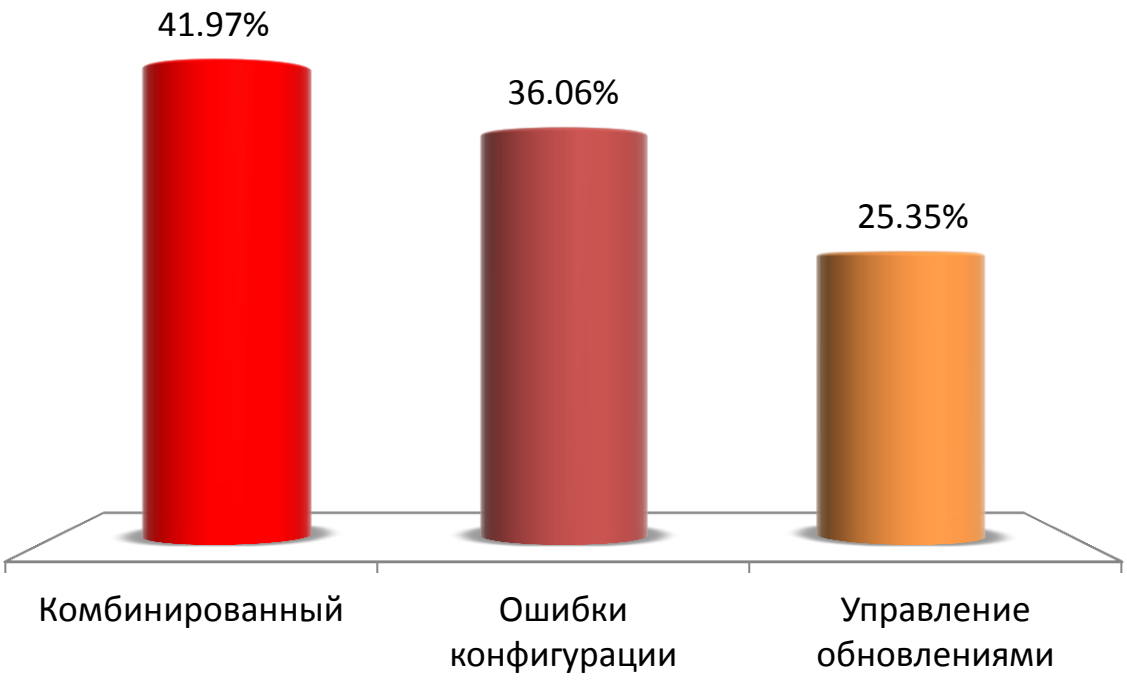

Рис. 18. Типы уязвимостей

5.5. Доля уязвимых компонентов АСУ ТП в разных странах

Наибольшая доля уязвимых компонентов АСУ ТП, которые видны из сети Интернет, приходится на Швейцарию. В этой стране уязвимы все подобные системы. На втором месте Чехия (86%), на третьем Швеция (67%)[5]. В России уязвима ровно половина (50%) интернет-доступных систем АСУ ТП.

Таблица 17. Доля уязвимых систем АСУ ТП в разных странах

Страна	Доля уязвимых АСУ ТП, %
Switzerland	100
Czech Republic	86
Sweden	67
Spain	63
Taiwan	60
United Kingdom	60
Russian Federation	50
Finland	50
Italy	42
United States	41
Poland	36
France	36
Netherlands	33
Austria	33
Korea	32
Canada	25
Germany	20
India	—
China	—

[5] В таблице 17 и на рис. 19 приведены страны с существенным количеством интернет-доступных систем АСУ ТП.

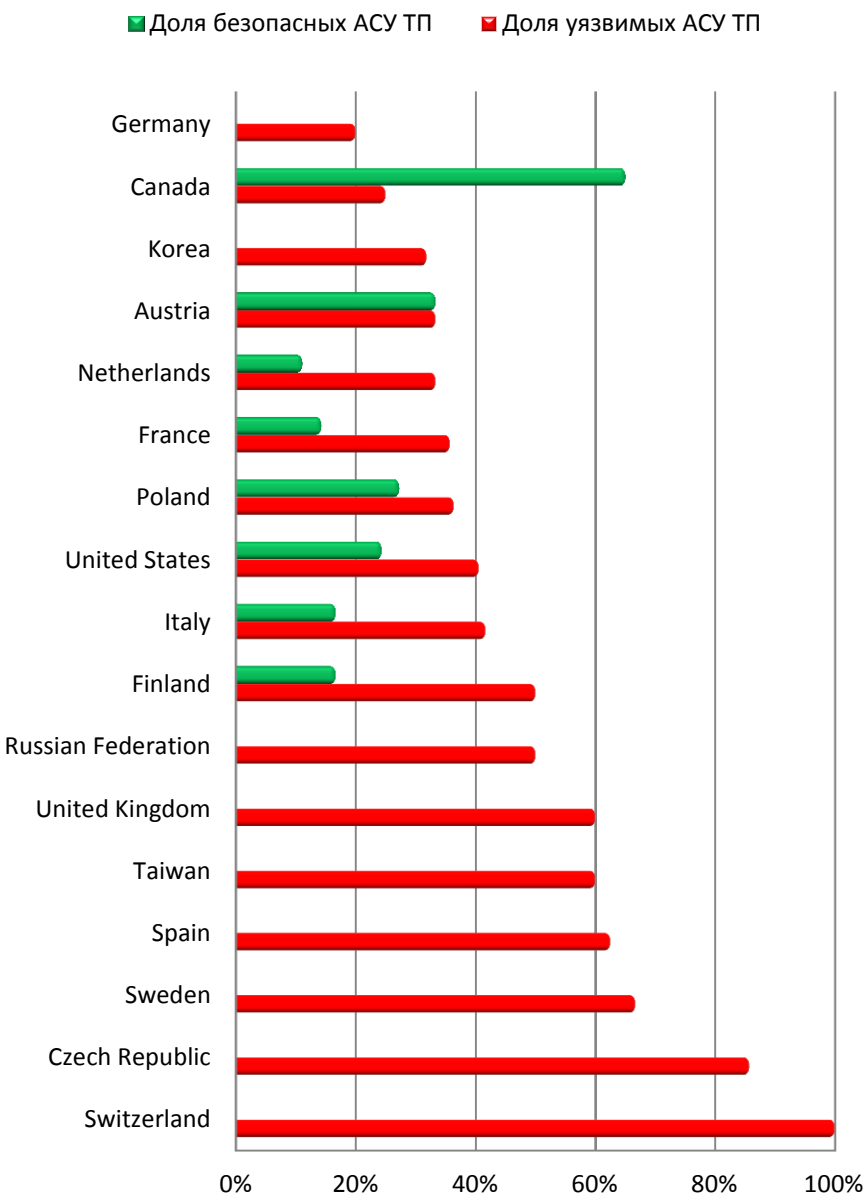

Рис. 19. Доля уязвимых компонентов АСУ ТП в разных странах

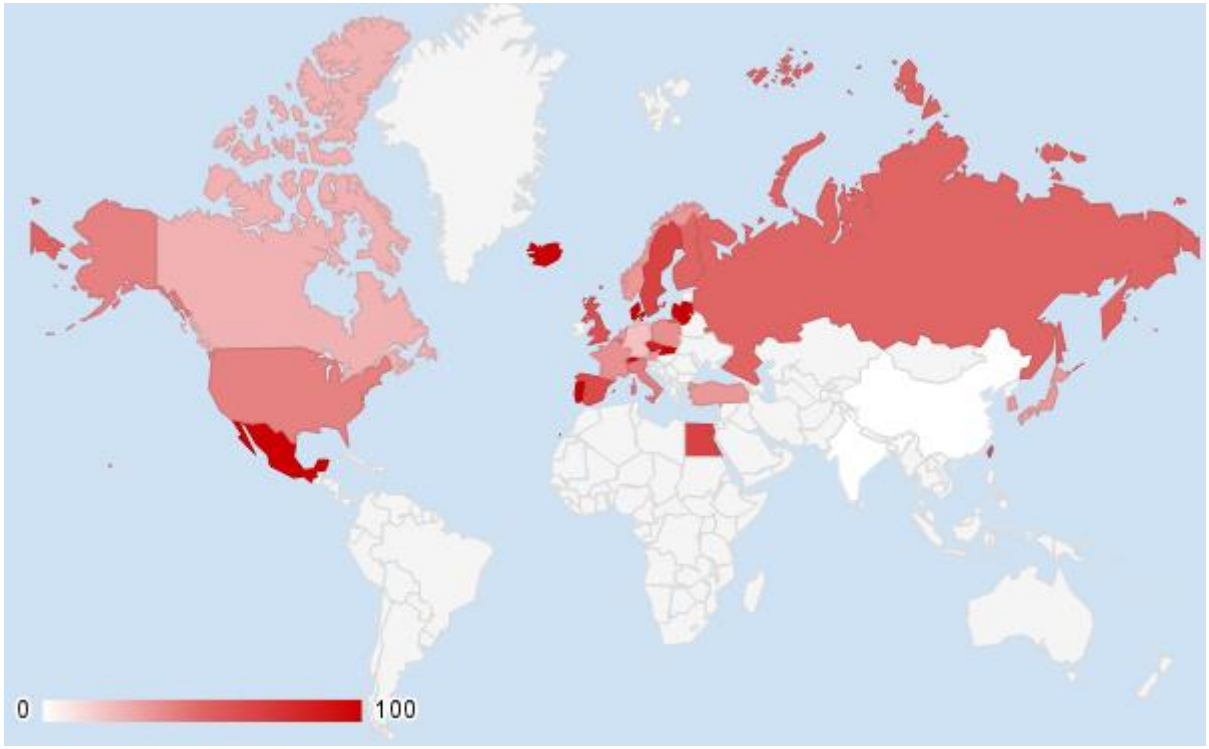

Рис. 20. Доля уязвимых компонентов АСУ ТП в разных странах

5.6. Доля уязвимых компонентов АСУ ТП в разных регионах

В Европе уделяют меньше всего внимания вопросам информационной безопасности АСУ ТП: 54% систем промышленной автоматизации, расположенных в данном регионе, являются уязвимыми и могут быть атакованы удаленно. На второй позиции Северная Америка (39%), на третьей — Азия (32%), где существенную роль, как видно из данных предыдущего раздела, играют небезопасные объекты на Тайване и в Южной Корее.

Таблица 18. Доля уязвимых компонентов АСУ ТП в разных регионах

Регион	Доля уязвимых компонентов, %
Europe	54
North America	39
Asia	32
MEA	30
India	—
South America	—

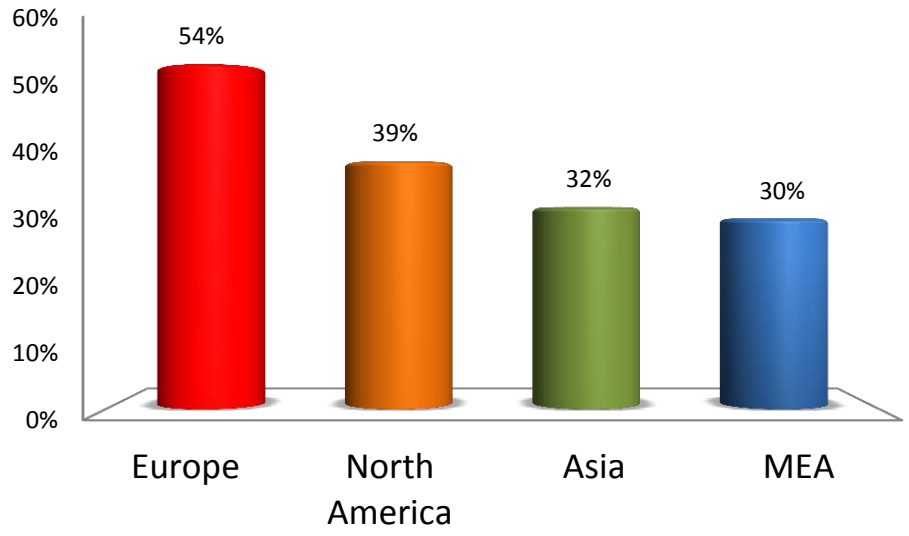

Рис. 21. Доля уязвимых компонентов АСУ ТП в разных регионах

6. Изменения

Благодаря конструктивной обратной связи сообщества www.asutpforum.ru в отчет было внесено ряд изменений. Изменения коснулись в основном первой части отчета (раздел №3 «Востребованность элементов систем АСУ ТП (SCADA) в России»), а также раздела №5.2. «Компоненты АСУ ТП».

7. О компании

Positive Technologies — российская компания-эксперт, лидер рынка систем анализа защищенности и соответствия стандартам, входит в топ-10 ведущих мировых игроков в сегменте Vulnerability Assessment*. В основе продуктов и услуг компании — опыт крупнейшего в Европе исследовательского центра Positive Research, обладающего уникальными знаниями в сфере практической информационной безопасности. Продукты Positive Technologies — MaxPatrol и XSpider — обладают репутацией лучших разработок в этой области. Компания выступает организатором международного форума Positive Hack Days и создателем самого популярного русскоязычного ИБ-портала SecurityLab.ru. Более подробную информацию можно получить на сайте www.ptsecurity.ru.

* По данным отчета IDC “Worldwide Security and Vulnerability Management 2012—2016 Forecast and 2011 Vendor Shares”.

www.ptsecurity.ru
pt@ptsecurity.ru
+7 (495) 744 01 44