Безопасность SCADA систем в промышленности.

Павлов С.Н.
СибГАУ им. академика М.Ф. Решетнева
Красноярск, Россия

Современная АСУ ТП (автоматизированная система управления технологическим процессом) представляет собой многоуровневую человеко-машинную систему управления. Создание АСУ сложными технологическими процессами осуществляется с использованием автоматических информационных систем сбора данных и вычислительных комплексов, которые постоянно совершенствуются по мере эволюции технических средств и программного обеспечения, но с увеличением технических средств в SCADA системах, растет и количество уязвимостей в них, которые могут использоваться киберпреступниками.

На сегодняшний день, после произошедших инцидентов в производстве, и нашумевших вредоносных программ (Stuxnet, Flame, DQ, и т.д.) поражавших SCADA системы, остро стоит вопрос о защищенности промышленных АСУ ТП.

Для оценки уровня опасности различных угроз АСУ, необходимо оценить степень проникновения различных производителей SCADA систем на Российский рынок. По данным портала http://www.controlglobal.com/, по состоянию на июнь 2013 года, доли различных производителей распределены следующим образом:

Производители ПЛК:

Таблица 1 – доли рынка производителей ПЛК

Производитель	**%**
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	23,7

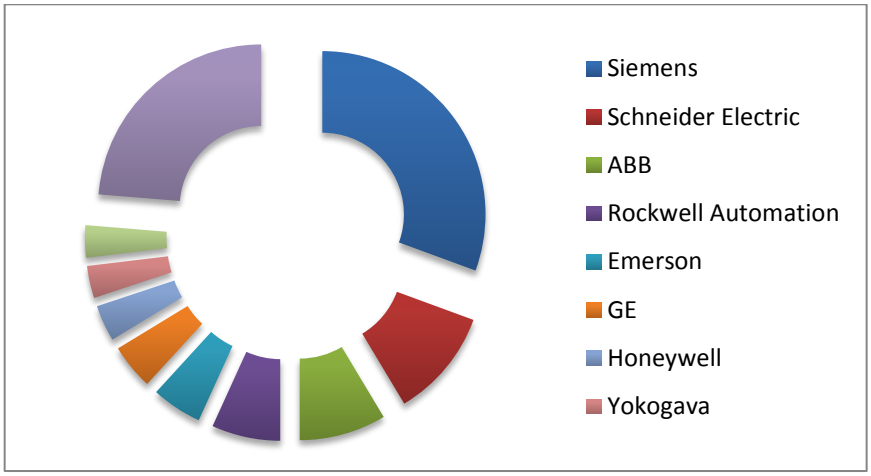

Рисунок 1 – диаграмма распределения рынка производителями ПЛК

Производители ПО SCADA систем:

Таблица 2 – доли рынка интеграции SCADA систем различных производителей

Производитель	**%**
STEP7	15
WinCC	14
InTouch	14
PCS7	14
Genesis	12
WinCC Flexible	11
Trace Mode	8
Rsview	8
Citect	2
Другие	1

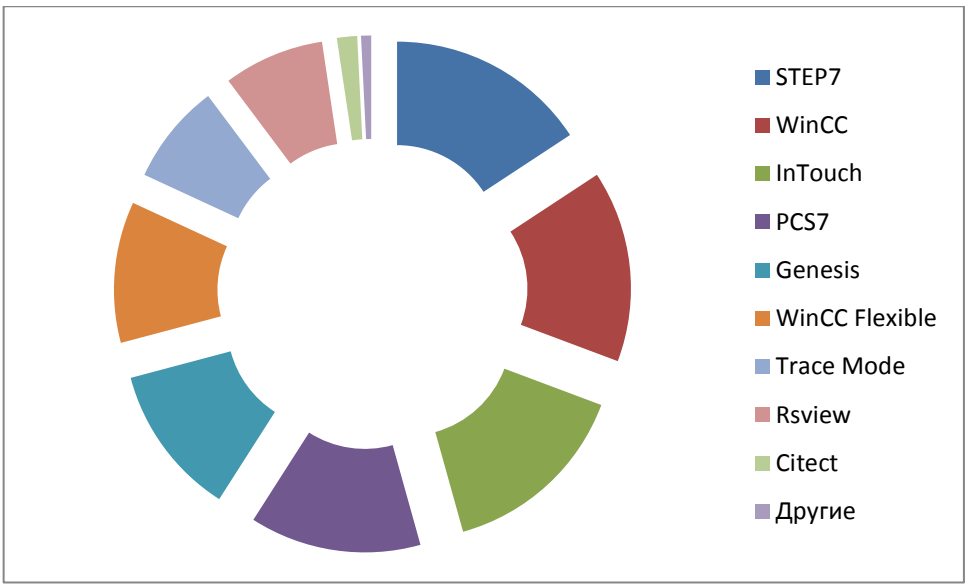

Рисунок 2 – диаграмма распределения рынка производителями SCADA

Большую долю рынка, среди используемых операционных систем для реализации АСУ ТП, занимают системы семейства Microsoft Windows, на втором месте системы семейства Unix и лишь незначительную часть занимают операционные системы реального времени QNX и FreeRTOS, среди СУБД лидерами рынка являются: Oracle, MySQL и MS SQL Server.

За период 2005-2010 г. было обнаружено и устранено 9 уязвимостей SCADA систем, а после того, как 17 июня 2010 года была обнаружена троянская программа win32/Stuxnet, резко возрос интерес к системе безопасности АСУ ТП, как со стороны аналитиков информационной безопасности, так и со стороны киберпреступников, итогом такого интереса стало открытие в 2011 году 64 новых уязвимостей, в 2012 году 117, а за 10 месяцев 2013 года их количество превысило 150. Некоторые производители ПО вплотную занялись устранением уязвимостей своих продуктов. Так, например фирма Siemens организовала специализированный отдел безопасности SCADA и HMI, задача которого является обнаружение и устранение уязвимостей.

Взглянув на график распределения уязвимостей по типам (рисунок 3), можно сделать вывод, что почти 50% известных уязвимостей позволяет злоумышленнику инициировать выполнение вредоносного кода на удаленной машине, что безусловно является высоким уровнем риска.

Таблица 3 – распределение по типам уязвимости

Тип уязвимости	%
Buffer Overlow	36
Authentication/Key Management	22,9
Remote code Execution	13,1
Web(server-side)	10,9
Web(client-side)	9,1
DoS/Data integrity	5,7
Local privilege escalation	2,3

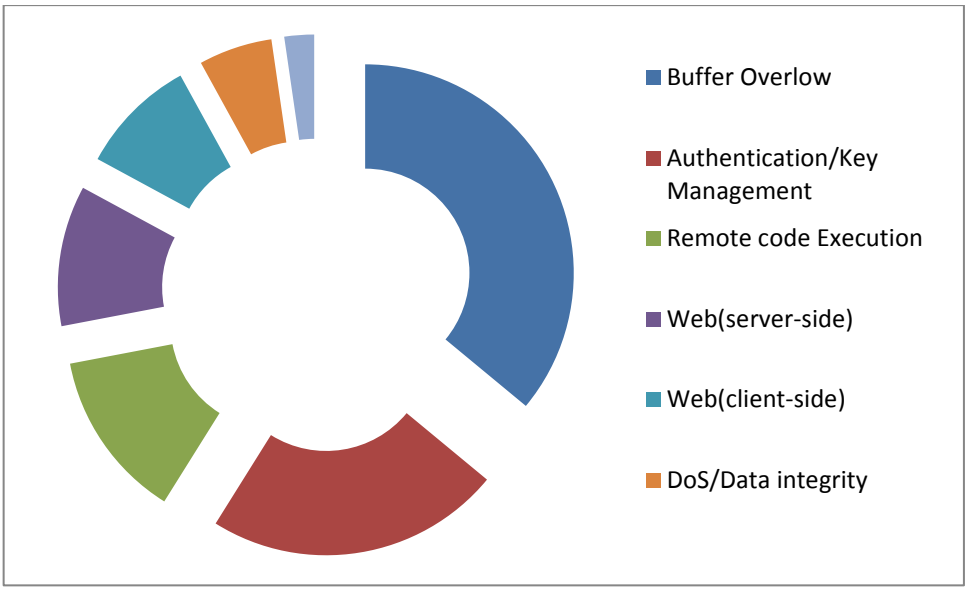

Рисунок 3 – распределение по типам уязвимости

Еще одной большой проблемой является незащищенность большинства протоколов обмена данными между SCADA и PLC, которые вообще не подразумевают какую либо аутентификацию и авторизацию пользователя или оборудования, что приводит к таким последствия как: любое появившееся устройство в технологической цепи может не только получать, но и выдавать управляющие команды на любое другое устройство в данной сети.

Также не способствуют улучшению ситуации и сами производители ПО SCADA систем и PLC, зачастую они записывают служебные логины и пароли, SSH и SSL ключи в самих ПЛК, что может способствовать подмене компонентов системы злоумышленниками, а также производители в большинстве случаев закладывают аппаратные и программные возможности

удаленного администрирования, однако конфигурирование этих параметров сами не производят, оставляя эту прерогативу за конечным пользователем, в свою очередь пользователь зачастую оставляет эти настройки по умолчанию, в результате чего, вся АСУ ТП доступна из интернета, и имеется возможность несанкционированного подключения, и изменения параметров всей системы.

Исходя из этого, можно сделать вывод, что современные АСУ ТП, уязвимы перед киберпреступниками, они могут быть взломаны с целью кражи конфиденциальной или коммерческой информации, либо внесены критические изменения в программу с целью отказа всего технологического оборудования и его поломки, могут неверно информировать оператора с целью принятия неверного решения и привести к аварийной ситуации.

Таким образом, на сегодняшний день назрела необходимость в создании решений, способных обеспечить надежный уровень защиты, в первую очередь, важных промышленных объектов, которые давали бы гарантии безопасности всей АСУ ТП.

Список литературы

1. Андреев, Е.Б. SCADA-системы: взгляд изнутри / Е.Б. Андреев, Н.А. Куцевич, О.В. Синенко // М.: Издательство «РТСофт», 2004. – 176 с.: ил.

2. Вилкомир, С.А. Комплекс программ для оценки надежности систем автоматизации электростанций. / С.А. Вилкомир, С.В. Виноградская, М.А. Ястребенецкий // Приборы и системы управления. 1994.- №7- С.32-36

3. Ицкович, Э.Л. Опыт использования открытых SCADA-программ / Э.Л. Ицкович, Ю.А. Соловьев, И.В. Мурзенко // Журнал «Промышленные АСУ и контроллеры». № 11 – Москва, 1999. – С. 36-38.

4. Wilamowski B.M., Industrial Communication Systems / Wilamowski B.M., Irwin J.D. // CRC Press, 2011. – 909 p.