I.A. Korsakov
GRCC Presidential Property Managenet Department of the Russian Federation, Ryabinovaya 43, Moscow, 121471, Russia, e-mail: korsakov2201@gmail.com, ORCID 0000-0003-0109-6756

The Method of Assessment of Impacts of a Cyberattacks on the Industrial Process

Keywords: industrial Ethernet, Programmable logic controller, PLC, network security, STUXNET, SCADA systems.

The rapid development of modern information management technology leads to the emergence of new aspect of their security. In particular, special importance has acquired the co-called problems of industrial cyber-security, gradually allocated in independent field of scientific and technical research. In recent years, the number of attacks on industrial objects has increased significantly. This is according by ICS-CERT reports for 2014–2015.

Several incidents that have received wide press coverage are related with cybersecurity issues. For example, the STUXNET virus, which affects Siemens industrial systems. STUXNET caused serious damage to Iran's nuclear program by exploiting vulnerabilities of the operating system and the so-called «human factor». There are a number of modified viruses capable of carrying out successful attacks on various industrial networks based on STUXNET architecture. Siemens is one of the key industrial equipment manufacturers in the world, so STUXNET is widespread and was even discovered at Russian NPP. Thus the security of the automated control systems, process control is critical now and its importance can not be underestimated.

One of the most devastating attacks on the possible damage is the diversion of the production process. Diversion of the process affects all levels of the process control system.

This article proposes assessment of consequences of performing each of the described attack's steps, determines the information possessed by the attacker after each phase of attack.

И.А. Корсаков
ГлавНИВЦ, Управление Делами Президента Российской Федерации, ул. Рябиновая, 43, Москва, 121471, Россия, e-mail: korsakov2201@gmail.com, ORCID 0000-0003-0109-6756

МЕТОДИКА ОЦЕНКИ ПОСЛЕДСТВИЙ КИБЕРАТАК НА ПРОИЗВОДСТВЕННЫЙ ПРОЦЕСС

Ключевые слова: промышленные сети, программируемые логические контроллеры, ПЛК, идентификация, сетевая безопасность, STUXNET, АСУ ТП.

Стремительное развитие современных информационных технологий управления приводит к появлению новых аспектов обеспечения их безопасности. В частности, особую актуальность приобрела проблема так называемой промышленной кибербезопасности, постепенно выделяемая в самостоятельную сферу научно-технических исследований. За последние годы количество атак на объекты промышленного производства значительно выросло. Об этом свидетельствуют данные отчетов ICS-CERT за 2014–2015 гг.

С вопросами кибербезопасности связано несколько инцидентов, получивших широкое освещение в прессе. Например, вирус STUXNET, поражающий промышленные системы Siemens. STUXNET нанес серьезный урон иранской ядерной программе, используя уязвимости операционной системы и «человеческий фактор». На основе STUXNET был разработан целый ряд модифицированных вирусов, способных осуществлять успешные атаки на различные промышленные сети. Siemens является одним из ключевых произ-

водителей промышленного оборудования в мире, поэтому STUXNET ожидаемо получил широкое распространение и в 2013 году был даже обнаружен на российской АЭС. Таким образом, безопасность систем автоматизированного контроля управления технологическим процессом является критической в настоящее время, и ее важность нельзя недооценивать.

Одной из наиболее разрушительных атак по возможному ущербу является диверсия производственного процесса. Диверсия производственного процесса затрагивает все уровни АСУ ТП.

Данная статья оценивает последствия совершения каждого из этапов описанной атаки, показывает дальнейшие пути развития атаки, определяет информацию, которой обладает злоумышленник после каждого из этапов атаки.

Введение

Промышленное производство в мире в настоящее время развивается быстрыми темпами. Почти во всех отраслях производства осуществляется переход к автоматизированному производству, которое управляется автоматизированными системами управления технологическим процессом (АСУ ТП). Также растет и объем производства. Это приводит к тому, что рынок программируемых логических контроллеров (ПЛК), являющихся основой систем АСУ ТП, растет огромными темпами. Например, промышленное производство в Азии выросло за последние пять лет на 52%, по данным IMSResearch (рис. 1). Помимо этого ожидается еще более бурный рост в следующие пять лет. Стремительное развитие современных информационных технологий управления приводит к появлению новых аспектов обеспечения их безопасности.

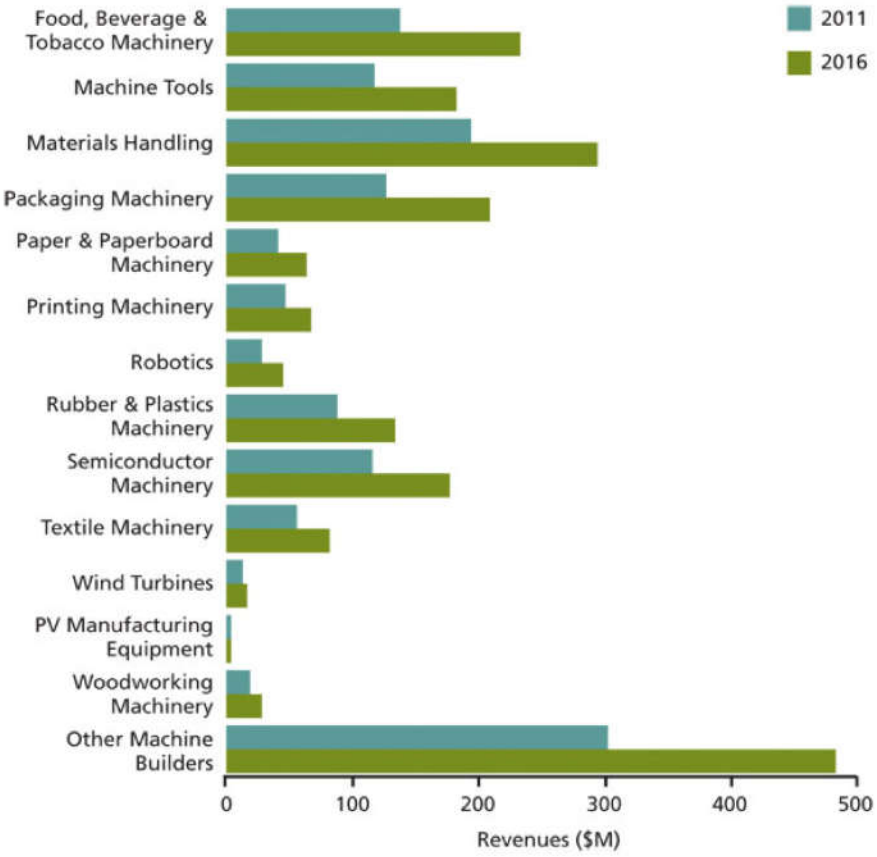

Рис.1. Объем рынка Азии программируемых логических контроллеров в сравнении 2011–2016 гг.

В частности, особую актуальность приобрела проблема так называемой промышленной кибербезопасности, постепенно выделяемая в самостоятельную сферу научно-технических исследований. С вопросами кибербезопасности связаны несколько инцидентов, получившие широкое освещение в прессе. Например, вирус STUXNET, поражающий промышленные системы Siemens [1, 2, 3]. STUXNET нанес серьезный урон иранской ядерной программе, используя уязвимости операционной системы и «человеческий фактор». Вирус поразил 1368 из 5000 центрифуг на заводе по обогащению урана и сорвал сроки запуска ядерной АЭС в Бушере. На основе STUXNET был разработан целый ряд модифицированных вирусов, способных осуществлять успешные атаки на различные промышленные сети [2, 4, 5]. Siemens является одним из ключевых производителей промышленного оборудования в мире, поэтому STUXNET ожидаемо получил широкое распространение и в 2013 году был даже обнаружен на российской АЭС [6]. В целом, STUXNET вызвал существенное увеличение количества атак на объекты промышленного производства [7]. Об этом свидетельствуют данные отчетов ICS-CERT за 2014–2015 гг., изображенные на рис. 2 [8].

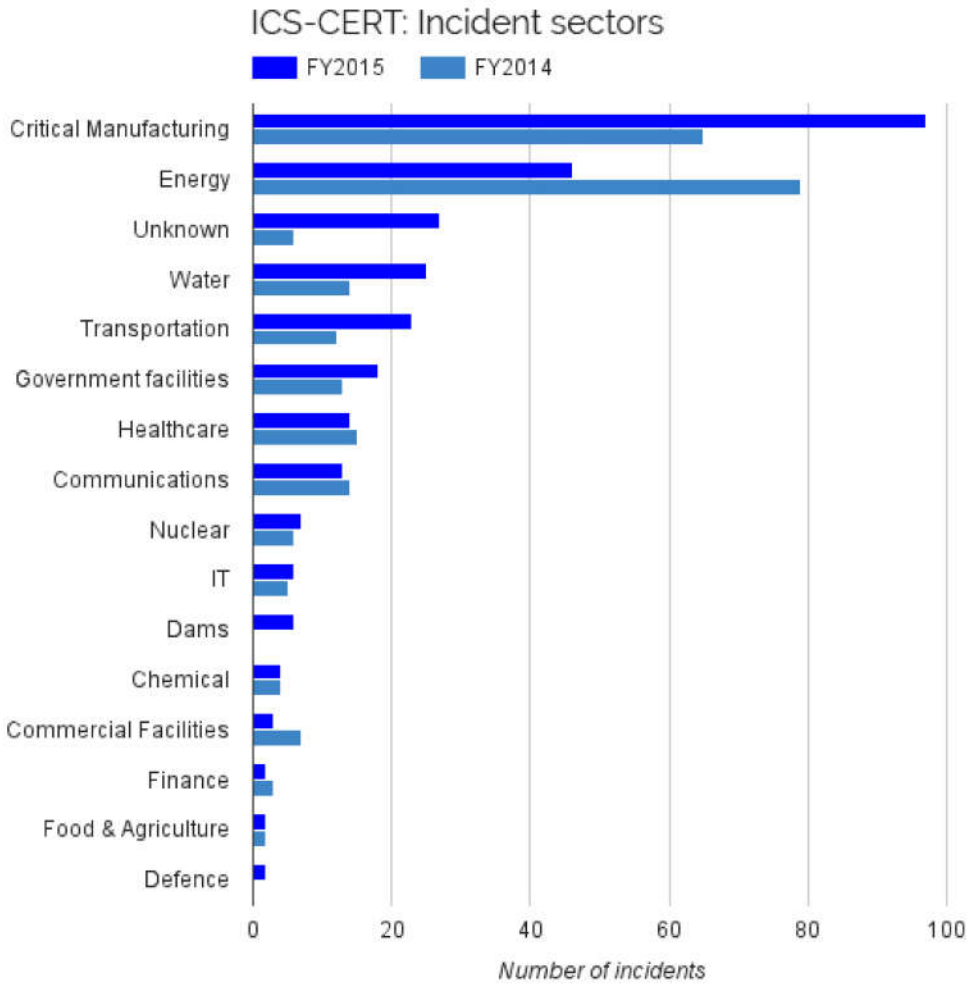

Рис. 2. Количество атак на промышленные объекты за 2014–2015 гг.

Таким образом, в настоящее время безопасность АСУ ТП является критически важной, и ее значимость нельзя недооценивать [9,10].

Программно-технический комплекс АСУ ТП делится на три уровня. Верхний уровень представляет собой АРМ и панели операторов, с установленными SCADA-системами. Средний уровень – это программируемые логические контроллеры (ПЛК), концентраторы, коммуникационные процессоры. Нижний уровень представлен различными устройствами – датчиками, исполнительными механизмами. Уровни связаны между собой управляющей программой, которая создается и изменяется на верхнем уровне, затем загружается на средний уровень – ПЛК, где ПЛК осуществляет управление нижним уровнем – различными оконечными устройствами, согласно загруженной управляющей программе.

Одной из наиболее разрушительных атак по возможному ущербу является диверсия производственного процесса. Диверсия производственного процесса затрагивает все уровни АСУ ТП. В общем случае такую атаку можно представить, как последовательность следующих действий злоумышленника.

1. Идентификация промышленного оборудования автоматизации.
2. Выявление управляющей программы.
3. Считывание управляющей программы.
4. Декомпиляция и внесение изменений в управляющую программу с целью разрушительного воздействия на оборудование (создание перегрузок и заведомо невыполнимых алгоритмов, порча оборудования).
5. Запись измененной программы на ПЛК.

Злоумышленник маскируется под SCADA-систему, чтобы идентифицировать промышленное оборудование среднего уровня (ПЛК). Затем, продолжая маскироваться под SCADA-систему, он осуществляет выявление и считывание управляющей программы с ПЛК. После этого программа декомпилируется, и в нее вносятся изменения с целью некорректного воздействия на оборудование нижнего уровня – осуществляется диверсия, в ходе которой оконечное оборудование может работать в условиях перегрузок, тем самым выполняя производственный процесс неправильно и некорректно или даже разрушая систему.

Данная статья оценивает последствия совершения каждого из этапов описанной атаки, показывает дальнейшие пути развития атаки, определяет информацию, которой обладает злоумышленник после каждого из этапов атаки.

1. Идентификация промышленного оборудования автоматизации

Злоумышленник выполняет идентификацию промышленного оборудования среднего уровня, с целью выявить управляющее устройство (ПЛК). В зависимости от применяемого стандарта построения сети передачи данных могут использоваться разные способы идентификации. Наиболее широко в настоящее время используются стандарты, основанные на технологии полевой шины (Fieldbus) и реализации промышленных протоколов на базе технологии Ethernet, имеющие общее название IndustrialEthernet. Доля IndustrialEthernet за последние годы стабильно увеличивается, о чем свидетельствуют данные недавнего исследования IHS/IMS («The World Market for IndustrialEthernet and FieldbusTechnologies – 2013 Edition») [11]. В 2016 г. количество развернутых в обрабатывающих отраслях промышленности сетевых узлов Ethernet удвоилось по сравнению с концом 2011 г. и составило 8,7 млн узлов IndustrialEthernet, тогда как пару лет назад их было 4,4 млн (рис. 3).

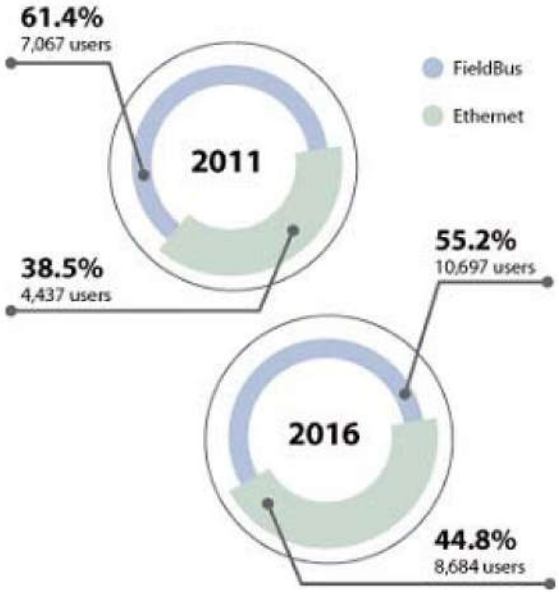

Рис. 3. Доля IndustrialEthernet в 2016 г. по сравнению с 2011 г.

Основной задачей идентификации является получение информации. Сбор информации осуществляется при помощи двух основных методов:

1) пассивный сбор информации;

2) активный сбор информации.

Идентификация промышленного оборудования автоматизации осуществляется всеми возможными способами сбора информации, в зависимости от перечня доступных условий.

Пассивный метод сбора информации основан на перехвате и дальнейшем анализе сетевых пакетов, передаваемых и получаемых на сетевом интерфейсе связи. При помощи пассивного метода возможно провести детализацию передаваемых данных, а также провести идентификацию сетевых объектов.

Активный метод идентификации оказывает непосредственное воздействие на объект с целью получения информации. Основным способом активной идентификации является сканирование портов. В настоящей статье описывается способ активной идентификации, основанный на сканировании портов. Протоколы, применяющие технологию IndustrialEthernet чаще всего, используют фиксированные порты для связи с ПЛК. Таким образом, можно определить не только протокол, но и производителя устройства. Соответствие протоколов и портов приведено в табл. 1.

После выполнения злоумышленником процедуры идентификации ПЛК и установления факта использования какого-либо промышленного протокола, возможен переход к следующему шагу.

Итогом данного шага является получение злоумышленником следующей информации: физические параметры промышленной сети, идентификаторы оборудования, существующего в данной сети, марка и модель программируемого контроллера, который управляет устройствами в данной сети. Используя полученную информацию, он способен перейти к следующему шагу реализации атаки. Еще одним важным последствием является возможность по определенному оборудованию выявить область производства, а значит, уже начать разработку плана осуществления диверсии производственного процесса.

Таблица 1. Перечень стандартных портов для протоколов на основе IndustrialEthernet

ABBRanger 2003	TCP:10307,10311,10364,10365,10407, 10409,10410,10412,10414,10415,10428, 10431,10432,10447,10449,10450,12316, 12645,12647,12648,13722,13724,13782, 13783,38589,38593,38600,38971,39129, 39278
BACnet/IP	UDP:47808
DNP3	TCP:20000 UDP:20000
Emerson/FisherROCPlus	TCP:4000 UDP:4000
EtherCAT	UDP:34980
EtherNet/IP	TCP:44818 UDP:2222,44818
ModBus	TCP:502 UDP:502
PROFINET	TCP:34962,34963,34964 UDP: 34962,34963,34964
SiemensSpectrumPowerTG	TCP:50001-50016,50018,50019,50020,50025, 50026,50027,50028,50110,50111 UDP:50020,50021
SafetyNET	TCP:40000 UDP:40000
SiemensS7 Communication	TCP: 102

Очевидно, что возможность реализации злоумышленником первого шага подобной атаки является следствием некорректной работы системы безопасности предприятия. Это может быть и отдел безопасности (в случае внутреннего нарушителя). Это может быть система обнаружения или система предотвращения вторжения в случае атаки извне. В любом случае, важным последствием является необходимость пересмотра системы безопасности предприятия или же ее части, ответственной за происшествие.

2. Выявление и считывание управляющей программы

Следующим шагом является подключение злоумышленником к ПЛК для получения диагностической информации о наличии или отсутствии управляющей программы. Выявление и считывание управляющей программы может быть осуществлено отправкой последовательности запросов специального вида, в соответствии с используемым протоколом и считыванием полученных ответов. Сделав вывод о наличии управляющей программы, злоумышленник может осуществить ее считывание.

Для выявления управляющей программы, злоумышленнику необходимо считать доступную для чтения память с ПЛК. Это возможно сделать следующим образом:

сформировать запрос специального вида на чтение определенного сегмента памяти;

прочитать ответ, представляющий собой дамп данной области;

повторить запрос для следующего сегмента памяти;

считать всю доступную память и создать двоичный файл дампа памяти ПЛК.

После этого задача выявления и считывания управляющей программы сводится к задаче поиска определенных заголовков в дампе памяти, полученном с ПЛК, что является тривиальной задачей.

Определенные разновидности ПЛК, например, ПЛК Siemens поддерживают запросы специального вида, являющиеся командами проприетарного протокола S7COMM [12], которые возвращают в качестве ответа список блоков управляющей программы. Также некоторые ПЛК поддерживают диагностическую информацию, которая содержит в себе информацию о наличии управляющей программы, списка сконфигурированного оборудования, использующегося в системе. Если это возможно, злоумышленнику достаточно лишь отправить специальный запрос и получить ответ заранее определенного вида, по которому можно сделать вывод о наличии управляющей программы.

После успешного считывания управляющей программы злоумышленником возможно провести ее декомпиляцию, для проведения идентификации производственного процесса. Большинство ПЛК хранят программу в блоках, имеющих несложную структуру.

Пример структуры блока программы, хранящейся на ПЛК Siemens серии S7-300, можно увидеть на рис.4.

Рис. 4. Пример структуры блока управляющей программы ПЛК Siemens S7-300

Заголовок и окончание блока, в свою очередь, имеют четко определенную структуру с определенным порядком параметров, которые достаточно легко поддаются обратной разработке.

Блок кода и блок данных представляют собой последовательность определенных последовательностей байтов, соответствующих вызовам различных функций, арифметическим операциям, операциям с памятью ПЛК. Такие последовательности тоже поддаются обратной разработке.

В результате этого возможна декомпиляция управляющей программы с целью идентификации производственного процесса. Когда злоумышленник определяет, какой технологический процесс выполняет полученная им управляющая программа, становится возможным внесение изменений в управляющую программу с целью осуществления диверсии производственного процесса. Такие изменения могут включать в себя преднамеренный вызов перегрузок оборудования, создание условий для работы, близких к критическим, или критических, отключение различных наблюдательных устройств (сенсоры, датчики), которые могут сигнализировать о неполадках в работе системы.

После этого необходимо осуществить компиляцию программы, и возможен переход к следующему шагу.

После выполнения данных шагов злоумышленник владеет всей информацией о технологическом процессе, диверсию которого он собирается осуществить. Помимо этого он обладает возможностью для осуществления изменения управляющей программы с целью внесения изменений в производственный процесс. Для успешной реализации всей атаки целиком, остается всего один шаг – внедрение измененной программы обратно на ПЛК. В случае возникновения подобного инцидента следует пересмотреть алгоритмы защиты управляющей программы, существующие на предприятии. Необходим пересмотр политики прав доступа пользователей к управляющей программе, механизмов идентификации/аутентификации, конфигурации ПЛК (в целях установки защиты на чтение управляющей программы).

3. Запись измененной программы

Запись измененной программы на ПЛК злоумышленником является процедурой, обратной процедуре считывания управляющей программы. Она сводится к перезаписи участка памяти, на котором находилась управляющая программа без изменений. Некоторые разновидности ПЛК поддерживают запросы определенного вида на перезапись определенного участка памяти, например, блока, управляющей программы. Таким образом, если изменения затронули небольшую часть управляющей программы, нет необходимости перезаписывать всю ее целиком.

После этого ПЛК начинает выполнять совсем другую программу, реализуя совершенно другой производственный процесс, что может привести к катастрофическим последствиям.

Итогом является срыв производственного процесса, вследствие выполнения оборудованием управляющей программы с внесенными изменениями.

Инцидент безопасности информации происходит в том случае, когда в результате атаки нарушается целостность, доступность или конфиденциальность информации. На промышленном предприятии, имеющем систему автоматизированного управления технологическим процессом, такая ситуация возможна, например, вследствие кибератаки. Главной целью расследования подобных инцидентов является смягчение последствий, если инцидент не удалось предотвратить. Это является критически важным для восстановления безопасности информации на промышленном объекте.

Заключение

Безусловно, данная проблема не является новой. Именно STUXNET показал, каким уязвимым является промышленное производство в настоящее время, и как легко, имея даже удаленный доступ к системе АСУ ТП, сорвать производство. Ряд производителей предприняли определенные меры по обеспечению безопасности SCADA-систем, целостности и конфиденциальности управляющей программы [13, 14]. Однако, последовательность действий злоумышленника, описанная в данной статье, остается актуальной и по настоящее время.

Средства обеспечения безопасности производственного процесса, предоставляемые производителями промышленных устройств, не являются достаточной защитой от атак подобного рода. Например, алгоритмы проверки целостности блока управляющей программы на ПЛК Siemens являются давно изученными, что позволяет злоумышленникам подделывать контрольные суммы блоков управляющей программы. Алгоритмы создания меток времени также являются очень простыми. Специфика промышленного производства не позволяет быстро внедрять изменения, пусть даже критические с точки зрения безопасности. Остановка некоторого производства, даже для обновления управляющего оборудования, влечет за собой серьезные затраты. Все это приводит к тому, что огромное количество промышленного оборудования автоматизации является уязвимым для атак подобного рода.

В качестве рекомендаций, можно отметить необходимость создания системы наблюдения за производственным процессом, не зависящую от АСУ ТП. Это может быть и дублирующая система, использующая второй набор датчиков и сенсоров для контроля над ситуацией. Это может быть система видеонаблюдения, при помощи которой можно наблюдать за функционированием АСУ ТП. Необходимо также контролировать аутентичность управляющей программы с заранее определенной периодичностью с целью отслеживания несанкционированных изменений.

СПИСОК ЛИТЕРАТУРЫ:

1. Falliere N., O'Murchu L. and Chien E/ (Symantec) // W32.Stuxnet Dossier, Ver 1.4 (February 2011).
2. The Real Story of Stuxnet. [Электронный ресурс] URL: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (Дата обращения 06.10.2016).
3. ICS Security Workspace. Security Analysis from Siemens S7 PLC CPU Buffer [Chinese].
4. Matrosov A., Rodionov E., Harley D., Malcho J. (ESET). Stuxnet Under the Microscope, Revision 1.1 (September 2010).
5. Freydman A.V. Stuxnet i promyshlennaya bezopasnost (Stuxnet and industrial safety) // Avtomatizatsiya v promyshlennosti, 2011, No 11, pp. 48–53.
6. Stuxnet infected Russian nuclear plant. [Электронный ресурс] URL: http://www.itnews.com.au/news/stuxnet-infected-russian-nuclear-plant-363578(Дата обращения 06.12.2016).
7. Peachey C. Is stuxnet a threat to NPPs? (2010) // NuclearEngineering International, 55 (676), pp. 22–23.
8. NCCIC/ICS-CERT. Year in Review National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team. FY 2015.
9. Cristea M., Groza B., Iacob M. Some security issues in Scalance wireless industrial networks (2011) Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011, art. no. 6046006, pp. 493–498.
10. Lau S., Klick J., Arndt S., Roth V. POSTER: Towards highly interactive honeypots for industrial control systems. (2016). Proceedings of the ACM Conference on Computer and Communications Security, 24-28-October-2016, pp. 1823-1825.
11. Powering-Up the Industrial Network. [Электронный ресурс] URL: http://www.panduit.com/ccurl/34/366/powering-up-ind-network,0.pdf (Дата обращения 06.12.2016).
12. What properties, advantages and special features does the S7 protocol offer? [Электронный ресурс] URL: https://support.industry.siemens.com/cs/document/26483647/what-properties-advantages-and-special-features-does-the-s7-protocol-offer-?dti=0&lc=en-WW (Дата обращения 06.12.2016).
13. SIMATIC WinCC / SIMATIC PCS 7: Information about Malware / Viruses / Trojan horses [Электронныйресурс] URL: https://support.industry.siemens.com/cs/document/43876783/simatic-wincc-simatic-pcs-7%3A-information-about-malware-viruses-trojan-horses?dti=0&lc=en-WW (Датаобращения 06.12.2016).
14. Chan R., Chow K.-P. Forensic analysis of a Siemens programmable logic controller. (2016) IFIP Advances in Information and Communication Technology, 485, pp. 117–130.

REFERENCES:

1. Falliere N., O'Murchu L. and Chien E/ (Symantec) // W32.Stuxnet Dossier, Ver 1.4 (February 2011).
2. The Real Story of Stuxnet. [Электронный ресурс] URL: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (Дата обращения 06.10.2016).
3. ICS Security Workspace. Security Analysis from Siemens S7 PLC CPU Buffer [Chinese].
4. Matrosov A., Rodionov E., Harley D., Malcho J. (ESET). Stuxnet Under the Microscope, Revision 1.1 (September 2010).
5. Freydman A.V. Stuxnet i promyshlennaya bezopasnost (Stuxnet and industrial safety) // Avtomatizatsiya v promyshlennosti, 2011, No 11, pp. 48–53.
6. Stuxnet infected Russian nuclear plant. [Электронный ресурс] URL: http://www.itnews.com.au/news/stuxnet-infected-russian-nuclear-plant-363578(Дата обращения 06.12.2016).
7. Peachey C. Is stuxnet a threat to NPPs? (2010) // NuclearEngineering International, 55 (676), pp. 22–23.
8. NCCIC/ICS-CERT. Year in Review National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team. FY 2015.
9. Cristea M., Groza B., Iacob M. Some security issues in Scalance wireless industrial networks (2011) Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011, art. no. 6046006, pp. 493–498.
10. Lau S., Klick J., Arndt S., Roth V. POSTER: Towards highly interactive honeypots for industrial control systems. (2016). Proceedings of the ACM Conference on Computer and Communications Security, 24-28-October-2016, pp. 1823-1825.
11. Powering-Up the Industrial Network. [Электронный ресурс] URL: http://www.panduit.com/ccurl/34/366/powering-up-ind-network,0.pdf (Дата обращения 06.12.2016).
12. What properties, advantages and special features does the S7 protocol offer? [Электронный ресурс] URL: https://support.industry.siemens.com/cs/document/26483647/what-properties-advantages-and-special-features-does-the-s7-protocol-offer-?dti=0&lc=en-WW (Дата обращения 06.12.2016).
13. SIMATIC WinCC / SIMATIC PCS 7: Information about Malware / Viruses / Trojan horses [Электронныйресурс] URL: https://support.industry.siemens.com/cs/document/43876783/simatic-wincc-simatic-pcs-7%3A-information-about-malware-viruses-trojan-horses?dti=0&lc=en-WW (Датаобращения 06.12.2016).
14. Chan R., Chow K.-P. Forensic analysis of a Siemens programmable logic controller. (2016) IFIP Advances in Information and Communication Technology, 485, pp. 117–130.