Игнатий А. Грачков
Федеральная служба по техническому и экспортному контролю,
105175, г. Москва, Старая Басманная, 17
e-mail: ignat958@gmail.com, https://orcid.org/0000-0001-6327-3530

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АСУ ТП: ВОЗМОЖНЫЕ ВЕКТОРА АТАКИ И МЕТОДЫ ЗАЩИТЫ

DOI: http://dx.doi.org/10.26583/bit.2018.1.09

Аннотация. Автоматизированные системы управления технологическими процессами (АСУ ТП) являются важнейшей частью промышленной инфраструктуры и используются на таких объектах, как нефте- и газопроводы, водораспределительные системы, электрические сети, атомные электростанции и производство. На сегодняшний день проблема обеспечения информационной безопасности АСУ ТП стоит довольно остро. Специалистами из разных стран проведено большое количество исследований в данной области. Способность злоумышленников обнаружить промышленные устройства, доступные через Интернет, и получать к ним несанкционированный доступ вызывает тревогу в кругах специалистов по информационной безопасности. Поисковик Shodan предоставляет атакующим мощный инструмент для идентификации автоматизированных системы управления и их компонентов и последующих злонамеренных воздействий на них. В данной статье дано описание типовой АСУ ТП; представлен общий анализ защищенности современных АСУ ТП; описаны возможные вектора атак на АСУ ТП; описан пример получения несанкционированного доступа к АСУ ТП с использованием поисковика Shodan; даны рекомендации по обеспечению информационной безопасности АСУ ТП.
Ключевые слова: автоматизированные системы управления, технологические процессы, АСУ ТП, информационная безопасность, защита информации, вектор атаки, Shodan.
Для цитирования. ***ГРАЧКОВ, Игнатий А.*** *ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АСУ ТП: ВОЗМОЖНЫЕ ВЕКТОРА АТАКИ И МЕТОДЫ ЗАЩИТЫ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 90-98, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1096>. Дата доступа: 19 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.09.*

Ignatiy A. Grachkov
FSTEC of Russia,
105175, Moscow, Staraya Basmannaya, 17
e-mail: ignat958@gmail.com, https://orcid.org/0000-0001-6327-3530

Information security of industrial control systems: possible attack vectors and protection methods

DOI: http://dx.doi.org/10.26583/bit.2018.1.09

Abstract. Industrial control systems are employed in numerous critical infrastructure assets including oil and gas pipelines, water distribution systems, electrical power grids, nuclear plants and manufacturing facilities. Today the problem of ensuring information security of the industrial control system is quite acute. Specialists from different countries conducted a large number of studies in this field. The ability of intruders to discover industrial devices accessible via the Internet and to obtain unauthorized access to them is of concern to information security professionals. The Shodan search engine provides the attacker with a powerful tool to identify industrial control systems and their components and subsequent malicious effects on them.
In this article the author describes the typical industrial control system, presents general analy-sis of the security of modern ICS and describes possible attack vectors on the ICS. An example of obtaining unauthorized access to industrial control systems using the Shodan search engine is described and recommendations how to ensure information security of the industrial control system are given.

Keywords: industrial control systems, technological processes, ICS, Information Security, data protection, attack vector, Shodan.

For citation. ***GRACHKOV, Ignatiy A.*** *Information security of industrial control systems: possible attack vectors and protection methods. IT Security (Russia), [S.l.], v. 25, n. 1, p. 90-98, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1096>. Date accessed: 19 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.09.*

Введение

Широкий интерес к защищенности промышленных систем возник не так давно, после серии инцидентов со специализированными компьютерными вирусами. Тогда выяснилось, что спецслужбы иностранных государств, конкурирующие корпорации или кибертеррористы могут использовать в своих целях недостаточное внимание к информационной безопасности автоматизированных систем управления технологическими процессами и их компонентов.

На сегодняшний день существует большое количество научных работ в области обеспечения информационной безопасности АСУ ТП [1-3]. Большой интерес у исследователей вызывают уязвимости различных компонентов АСУ ТП и возможность проведения атак на них [4-6]. Многие из уязвимых компонентов автоматизированных систем можно обнаружить напрямую из сети Интернет с помощью поисковика Shodan [7]. Одним из направлений научных изысканий в данной области также является анализ рисков информационной безопасности АСУ ТП [8]. Кроме того, много внимания уделяется сетевой безопасности автоматизированных систем управления [9-12]. По результатам исследования компании Positive Technologies, 54 % всех АСУ ТП уязвимы к различным атакам [13]. И причин столь плачевного положения дел - несколько. Во-первых, это консерватизм руководителей предприятий, которые нацелены на приоритетное обеспечение стабильности производственных процессов, а потому не желают рисковать, внося изменения (пусть даже связанные с безопасностью) в производственные системы. Во-вторых, это морально устаревшие решения, используемые в современных производственных комплексах. В-третьих, отсутствие высококвалифицированных специалистов в области обеспечения ИБ на производстве и КВО.

В отличие от уже привычных вирусов для персональных компьютеров и мобильных телефонов, деструктивное информационно-техническое воздействие на автоматизированные системы управления технологическими процессами несет огромную социальную опасность. Такое «информационное оружие» может привести к серьезным человеческим жертвам [14].

Возможные вектора атаки и их реализация в типовой АСУ ТП

Автоматизированная система управления технологическим процессом (АСУ ТП) - это совокупность технических и программных средств, предназначенных для автоматизации управления технологическим и промышленным оборудованием.

Структура типовой АСУ ТП представляет собой трехуровневую модель (разделение на уровни в соответствии с приказом ФСТЭК России №31) (рис. 1):

- На нижнем уровне располагаются исполнительные механизмы, датчики, приводы, регистраторы и индикаторы, связанные локальной сетью нижнего уровня.
- На среднем уровне находятся программируемые логические контроллеры (ПЛК), которые с помощью аналоговых подключений, полевых шин и проприетарных проколов связаны с устройствами нижнего уровня.
- На верхнем уровне могут располагаться автоматизированные рабочие места сотрудников, сервера, SCADA-системы и человеко-машинный интерфейс.

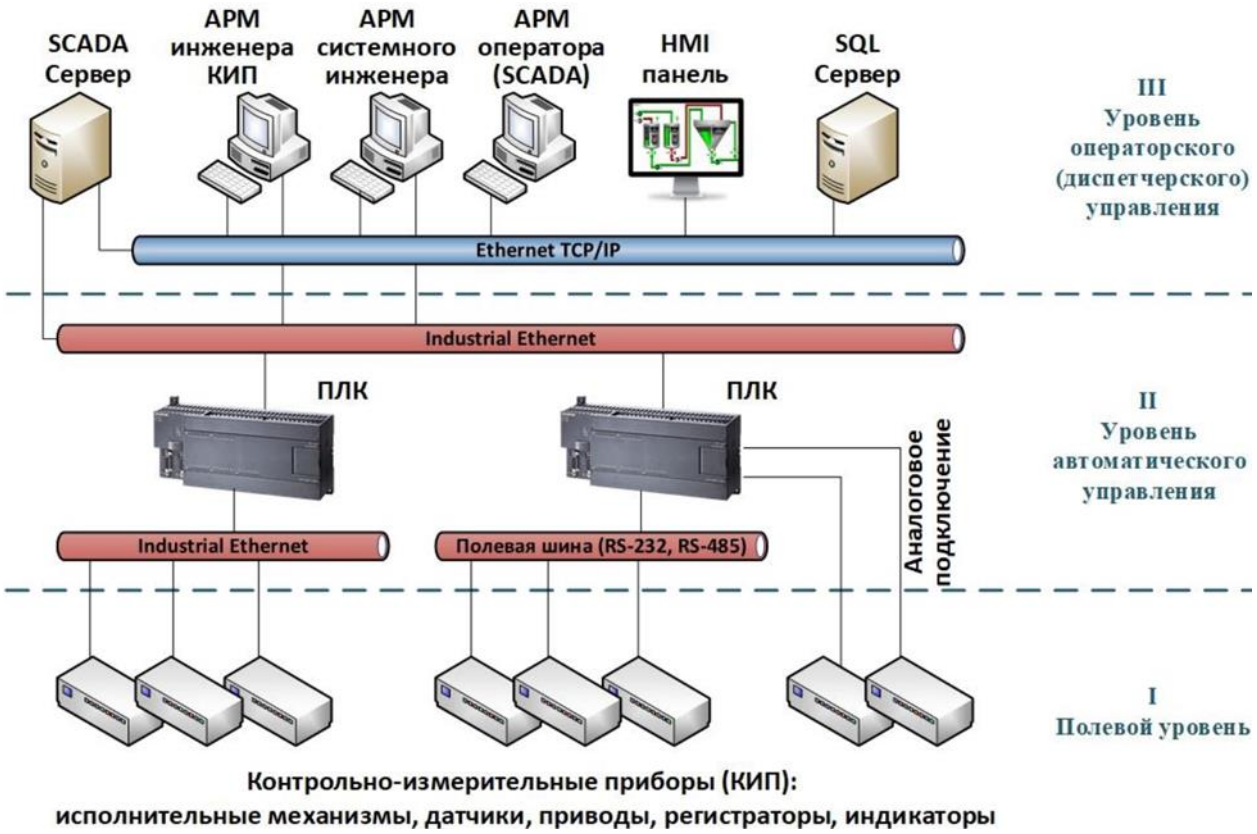

Рис. 1. Типовая архитектура АСУ ТП
(Fig.1. Structure of usual ICS)

Программные составляющие АСУ ТП:

- операционные системы реального времени;
- системы сбора данных и диспетчерского управления (SCADA).

Аппаратные составляющие АСУ ТП:

- программируемые логические контроллеры;
- датчики, регистраторы, привода и исполнительные механизмы;
- модули цифрового и/или человеко-машинного интерфейса;
- АРМ оператора и серверы системы;
- коммуникационные сети.

Перечень основных угроз АСУ ТП, отмеченных в реальных инцидентах:

- атаки на системы сбора данных и диспетчерского управления (SCADA);
- атаки на ПЛК с использованием их уязвимостей (неавторизованный доступ к фирменному программному обеспечению, пароль по умолчанию, удалённое изменение пароля и т. д.);
- атаки на инфраструктуру и операционные системы (троянские программы, вирусы, черви, ARP-спуфинг, DoS- и DDos-атаки);
- атаки на протоколы с использованием их уязвимостей;
- атаки на базы данных (SQL инъекция);
- другие атаки (переполнение буфера, отказ в доступе, отказ в управлении, отказ в представлении, подмена представления) [15].

Наибольшее количество уязвимостей среди компонентов АСУ ТП имеют SCADA-системы - 87% (процент уязвимых систем от их общего количества), далее следуют системы человеко-машинного интерфейса - 49%, реже обнаруживаются уязвимости в

программируемых логических контроллерах - 20%, и совсем редко в проприетарных протоколах - 1% [13].

На сегодняшний день огромное количество различных компонентов автоматизированных систем управления технологическими процессами доступны из сети Интернет, о чем свидетельствуют результаты поиска с использованием поисковика Shodan (рисунок 2). Shodan (https://www.shodan.io) посылает запрос на публично доступные IP-адреса и протоколирует информацию, полученную в ответ (название устройств, их тип, наличие веб-интерфейса и т.д.). В результате создается карта сети Интернет, с помощью которой можно искать устройства с сетевым интерфейсом или, установив нужные фильтры, смотреть за актуальным состоянием глобальной сети и изучать характер распространения уязвимостей [7].

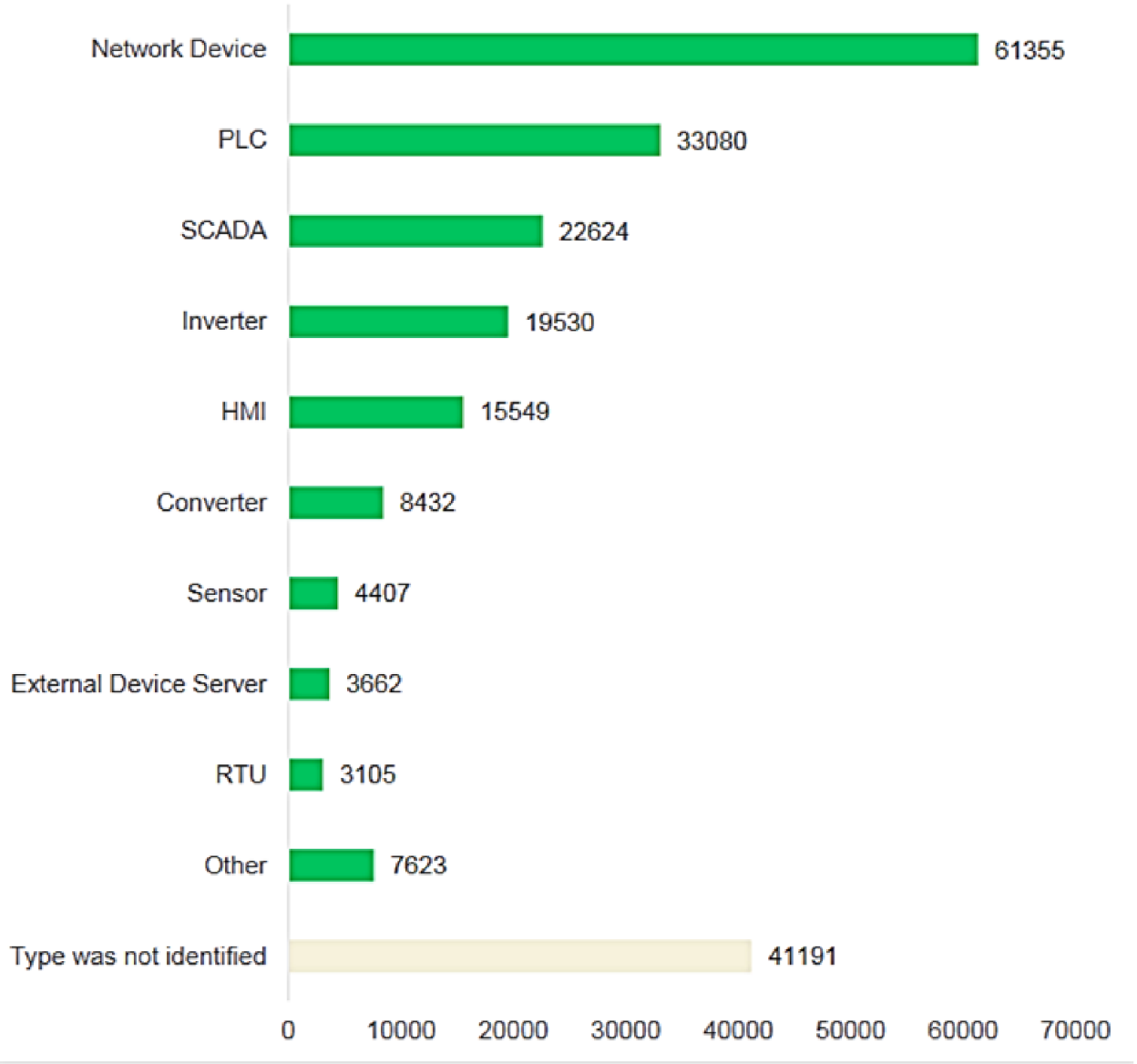

Рис.2. Количество доступных компонентов АСУ ТП из сети Интернет [16]
(Fig.2. Amount of available from the Internet components of ICS)

В качестве примера для практической реализации можно рассмотреть потенциальный вектор атаки на типовую АСУ ТП - доступ к проприетарному программному обеспечению с использованием аутентификационных данных «по умолчанию».

С помощью поисковика Shodan были найдены доступные из сети устройства i.LON SmartServer с открытым веб-интерфейсом (фильтр «200» в Shodan) - их обнаружилось 36

шт. (рисунок 3). Интернет-сервер i.LON SmartServer компании Echelon предназначен для управления сетями LonWorks и используется для автоматизации зданий, управления системами освещения, отопления, вентиляции и кондиционирования, позволяет подключать напрямую счетчики воды, электроэнергии и газа, а также применяется для централизованного энергетического менеджмента на территориально распределенных предприятиях.

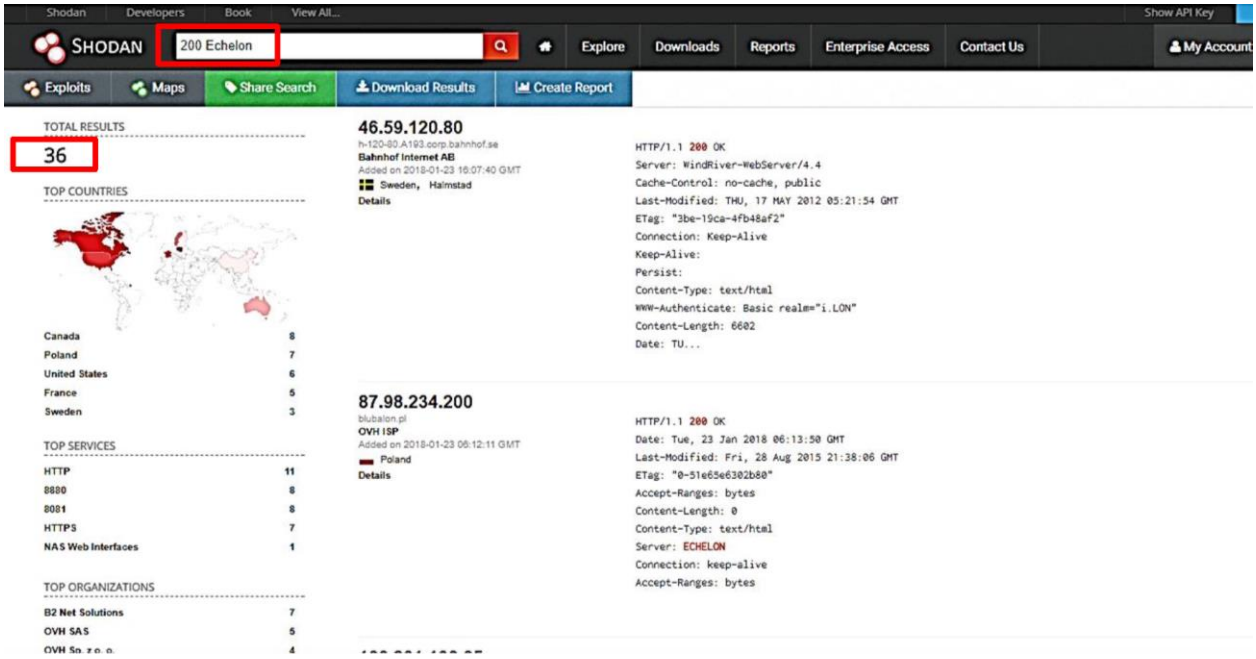

Рис.3. Результаты поиска в Shodan
(Fig.3. Results of Shodan search)

Далее был выбран интернет-серверы i.LON SmartServer, расположенной в Корее, с ip-адресом 1.212.147.219 (рисунок 4).

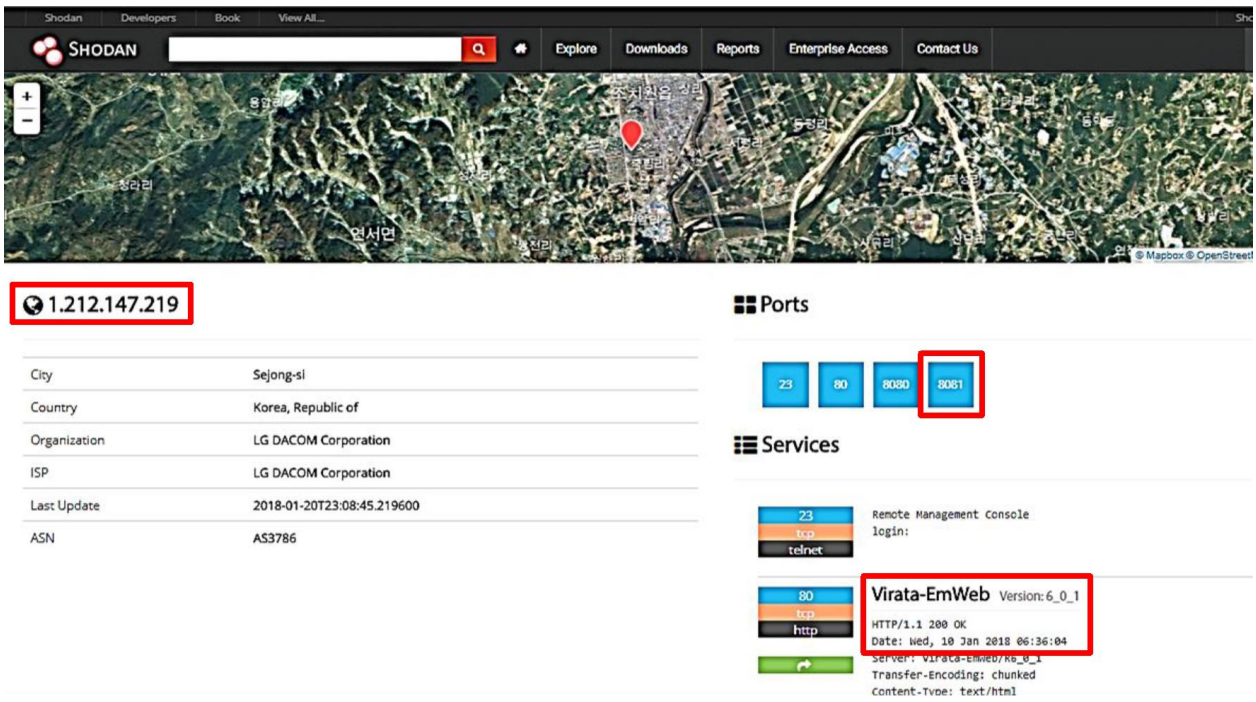

Рис.4. Устройство, доступное по адресу 1.212.147.219
(Fig.4. Device with 1.212.147.219 address)

Был выполнен переход по указанному адресу и обнаружено, что панель управления интернет-сервером защищена при помощи авторизации (рисунок 5).

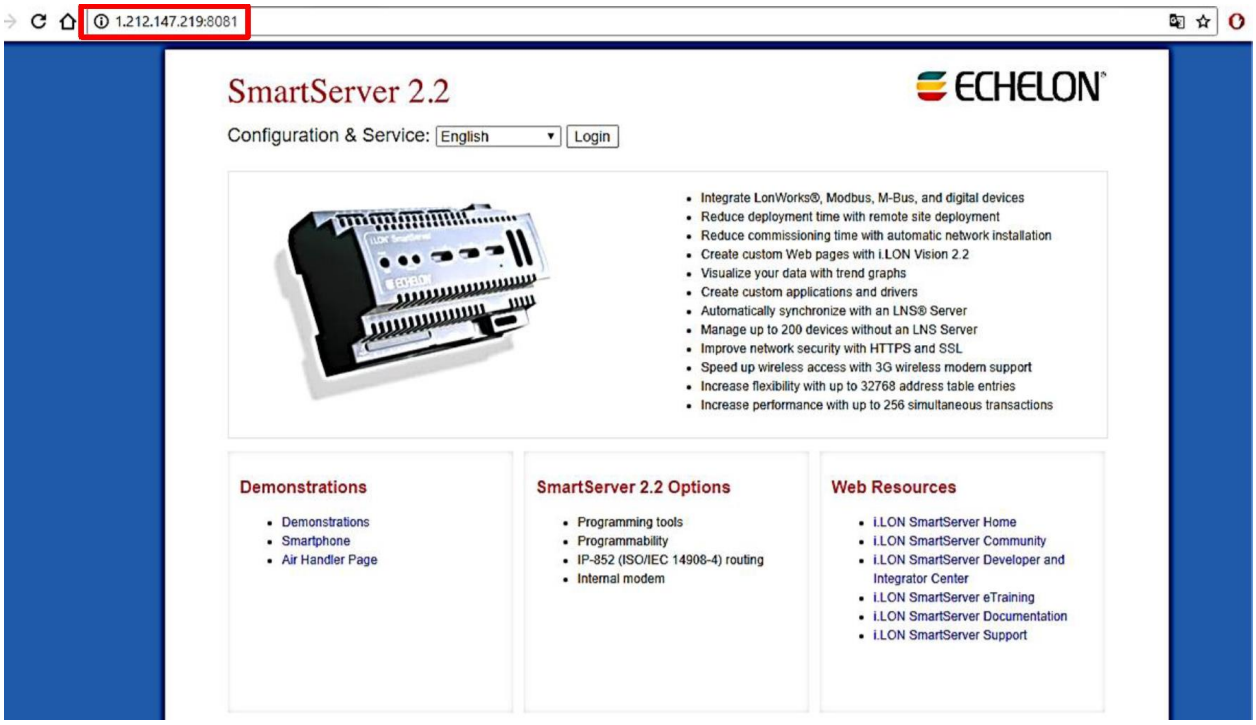

Рис.5. Окно авторизации на интернет-сервере
(Fig.5. Authorization window of the internet-server)

Для успешной авторизации на интернет-сервере с помощью базы логинов и паролей «по умолчанию» для различных компонентов SCADA-систем была подобрана пара логин/пароль для данного устройства (рисунок 6).

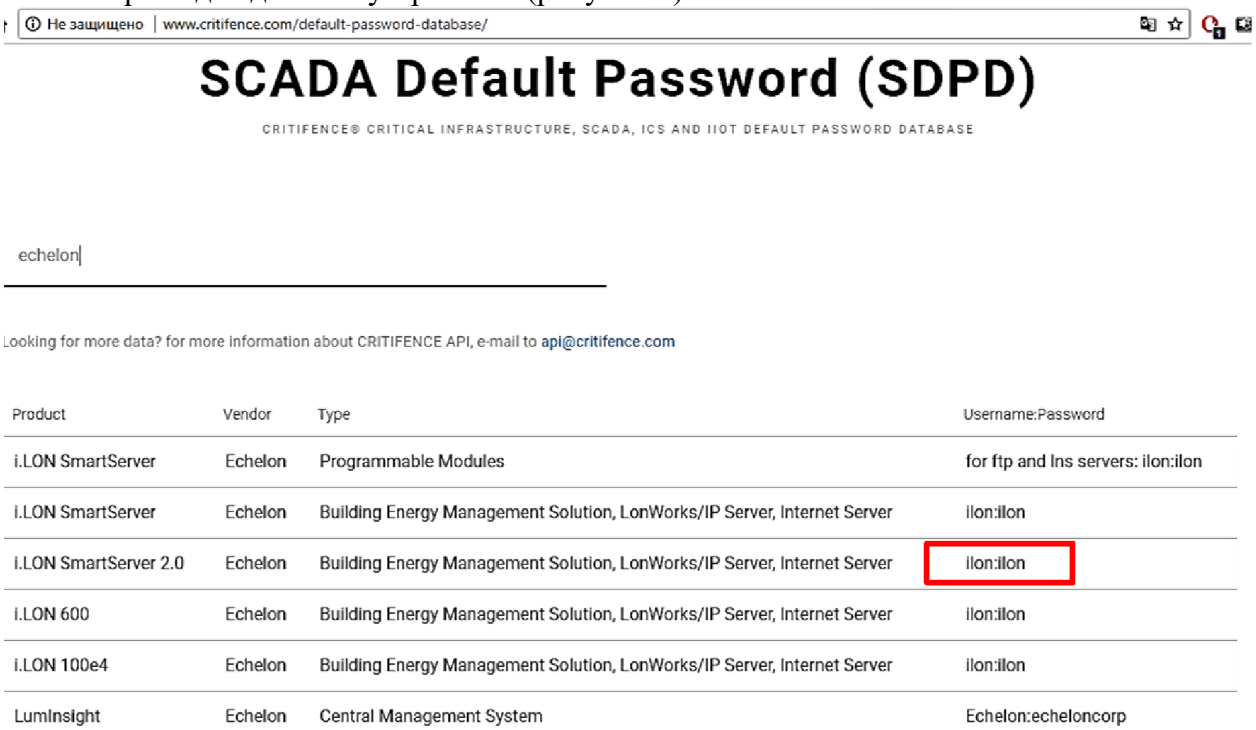

Рис.6. База логинов и паролей «по умолчанию» для различных компонентов SCADA-систем
(Fig.6. SCADA Default Password Database)

Далее был осуществлен успешный вход в консоль администратора интернет-сервера (рисунок 7). Используя консоль администратора, потенциальный злоумышленник может получить различные данные об устройстве, например, версию прошивки, и использовать соответствующие уязвимости, информация о которых находится в открытом доступе в сети Интернет.

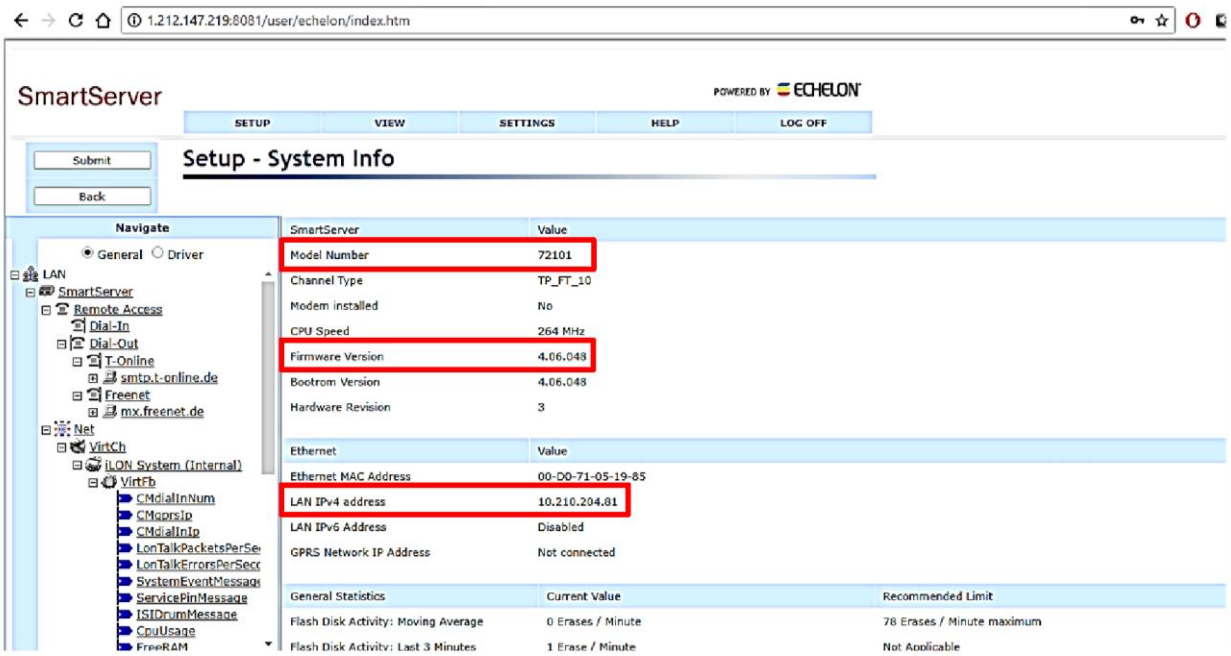

Рис.7. Информация об устройстве
(Fig.7. Information about device)

Также потенциальный злоумышленник может нарушить работу устройства, сменить пароль консоли управления и, тем самым, запретить доступ к нему системному администратору (рисунок 8).

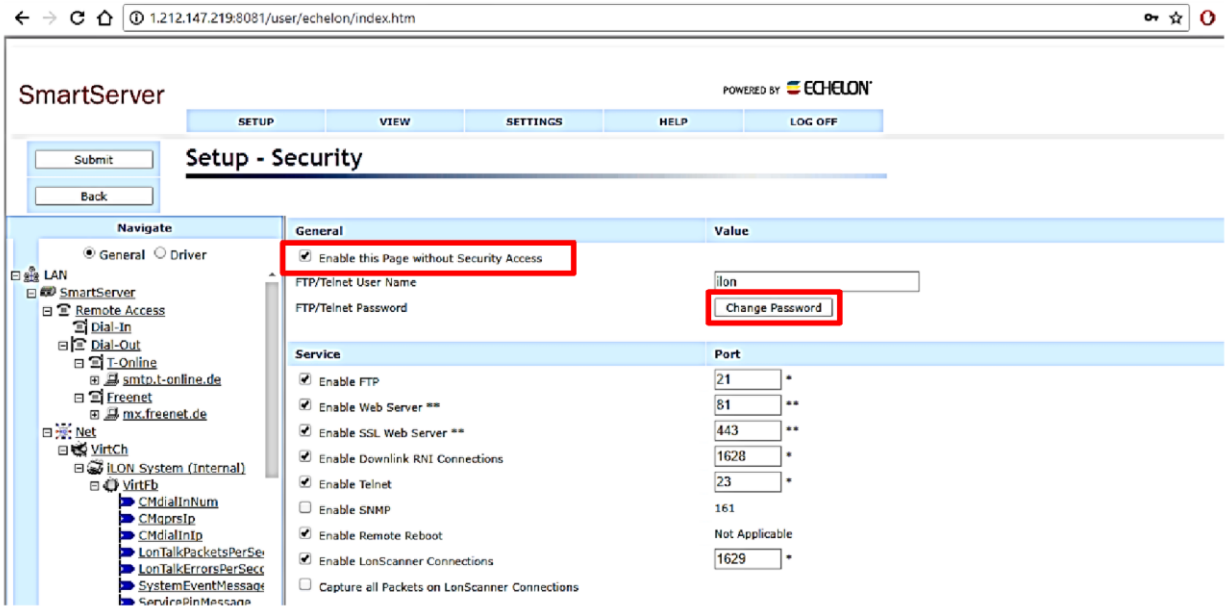

Рис.8. Страница управления паролем консоли
(Fig.8. Password management page)

В результате данного исследования ни одно устройство не пострадало. Данный эксперимент преследовал исключительно научные цели - показать реальность атак и простоту их реализации.

Заключение

Вышеописанный пример показал, что атаки такого типа реальны, легко реализуемы и могут касаться как обычных систем автоматизации зданий, которые используют интернет-сервер i.LON SmartServer для удаленного доступа, управления и конфигурирования устройств, так и предприятий, которые организуют свой производственный процесс с использованием данного оборудования (например – насосных станций). Последствия нарушения производственного процесса такого предприятия могут быть весьма масштабными.

Возможные способы защиты от атак данного типа:

- обязательная смена паролей «по умолчанию» и увеличение их сложности;
- своевременное обновление прошивок оборудования до последней версии;
- периодический мониторинг уязвимостей и обновлений программного обеспечения, устраняющих их.

На сегодняшний день подход производителей промышленного программного обеспечения и оборудования к исправлению уязвимостей, а также ситуация с устранением известных уязвимостей в автоматизированных системах, развернутых на предприятиях, остаются плачевными. Как результат, подавляющее большинство автоматизированных систем управления технологическими процессами в данный момент остаются уязвимы к атакам.

Данное исследование преследует цель показать, насколько легко можно получить доступ к компонентам реальной автоматизированной системы управления, а также пролить свет на то, какие негативные последствия могут быть этим вызваны.

СПИСОК ЛИТЕРАТУРЫ:

1 Sajid Nazir, Shushma Patel, Dilip Patel, Assessing and augmenting SCADA cyber security: A survey of techniques, Computers & Security, Volume 70, September 2017, Pages 436-454. DOI: 10.1016/j.cose.2017.06.010.
2 A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, SCADA security in the light of Cyber-Warfare, Computers & Security, Volume 31, Issue 4, June 2012, Pages 418-436. DOI: 10.1016/j.cose.2012.02.009.
3 Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review, Available online, January 2018. DOI: 10.1016/j.clsr.2017.12.004.
4 Danny Bradbury, SCADA: a critical vulnerability, Computer Fraud & Security, Volume 2012, Issue 4, April 2012, Pages 11-14. DOI: 10.1016/S1361-3723(12)70030-1.
5 Christopher M. Talbot, Michael A. Temple, Timothy J. Carbino, J. Addison Betances, Detecting rogue attacks on commercial wireless Insteon home automation systems, Computers & Security, In press, cor-rected proof, Available online 13 October 2017. DOI: 10.1016/j.cose.2017.10.001.
6 Igor Nai Fovino, Andrea Carcano, Marcelo Masera, Alberto Trombetta, An experimental investigation of malware attacks on SCADA systems, International Journal of Critical Infrastructure Protection, Volume 2, Issue 4, December 2009, Pages 139-145. DOI: 10.1016/j.ijcip.2009.10.001.
7 Roland Bodenheim, Jonathan Butts, Stephen Dunlap, Barry Mullins, Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices, International Journal of Criti-cal Infrastructure Protection, Volume 7, Issue 2, June 2014, Pages 114-123. DOI: 10.1016/j.ijcip.2014.03.001.
8 H. Abdo, M. Kaouk, J.-M. Flaus, F. Masse, A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis, Computers & Security, Volume 72, January 2018, Pages 175-195. DOI: 10.1016/j.cose.2017.09.004.
9 Luis Martín-Liras, Miguel A. Prada, Juan J. Fuertes, Antonio Morán, Manuel Domínguez, Comparative analysis of the security of configuration protocols for industrial control devices, International Journal of Critical Infrastructure Protection, Volume 19, December 2017, Pages 4-15. DOI: 10.1016/j.ijcip.2017.10.001.
10 Cristina Alcaraz, Javier Lopez, Kim-Kwang Raymond Choo, Resilient interconnection in cyber-physical control systems, Computers & Security, Volume 71, November 2017, Pages 2-14. DOI: 10.1016/j.cose.2017.03.004.
11 Niv Goldenberg, Avishai Wool, Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, International Journal of Critical Infrastructure Protection, Volume 6, Issue 2, June 2013, Pages 63-75. DOI:

10.1016/j.ijcip.2013.05.001.
12 Rafael Ramos Regis Barbosa, Ramin Sadre, Aiko Pras, Flow whitelisting in SCADA networks, Interna-tional Journal of Critical Infrastructure Protection, Volume 6, Issues 3–4, December 2013, Pages 150-158. DOI: 10.1016/j.ijcip.2013.08.003.
13 Грицай, Г., Тиморин, А., Гольцев, Ю. Positive Technologies. Безопасность промышленных систем в цифрах [Электронный ресурс] Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/SCADA-analytics-rus.pdf (дата обращения 23.01.2018).
14 Михайлов, Д.М., Жуков, И.Ю., Шеремет, И.А. Защита автоматизированных систем от информационно-технологических воздействий. – М.: НИЯУ МИФИ, 2014. – 184 с.
15 Пищик, Б.Н. Безопасность АСУ ТП // ЖВТ. 2013. №. С.170-175
16 Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S., Timorin, A., Industrial control systems and their online availability. Access mode: https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Availability_Statistics.pdf.

REFERENCES:

[1] Sajid Nazir, Shushma Patel, Dilip Patel, Assessing and augmenting SCADA cyber security: A survey of techniques, Computers & Security, Volume 70, September 2017, Pages 436-454. DOI: 10.1016/j.cose.2017.06.010.
[2] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, SCADA security in the light of Cyber-Warfare, Computers & Security, Volume 31, Issue 4, June 2012, Pages 418-436. DOI: 10.1016/j.cose.2012.02.009.
[3] Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review, Available online, January 2018. DOI: 10.1016/j.clsr.2017.12.004.
[4] Danny Bradbury, SCADA: a critical vulnerability, Computer Fraud & Security, Volume 2012, Issue 4, April 2012, Pages 11-14. DOI: 10.1016/S1361-3723(12)70030-1.
[5] Christopher M. Talbot, Michael A. Temple, Timothy J. Carbino, J. Addison Betances, Detecting rogue attacks on commercial wireless Insteon home automation systems, Computers & Security, In press, cor-rected proof, Available online 13 October 2017. DOI: 10.1016/j.cose.2017.10.001.
[6] Igor Nai Fovino, Andrea Carcano, Marcelo Masera, Alberto Trombetta, An experimental investigation of malware attacks on SCADA systems, International Journal of Critical Infrastructure Protection, Volume 2, Issue 4, December 2009, Pages 139-145. DOI: 10.1016/j.ijcip.2009.10.001.
[7] Roland Bodenheim, Jonathan Butts, Stephen Dunlap, Barry Mullins, Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices, International Journal of Critical Infrastructure Protection, Volume 7, Issue 2, June 2014, Pages 114-123. DOI: 10.1016/j.ijcip.2014.03.001.
[8] H. Abdo, M. Kaouk, J.-M. Flaus, F. Masse, A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis, Computers & Security, Volume 72, January 2018, Pages 175-195. DOI: 10.1016/j.cose.2017.09.004.
[9] Luis Martín-Liras, Miguel A. Prada, Juan J. Fuertes, Antonio Morán, Manuel Domínguez, Comparative analysis of the security of configuration protocols for industrial control devices, International Journal of Critical Infrastructure Protection, Volume 19, December 2017, Pages 4-15. DOI: 10.1016/j.ijcip.2017.10.001.
[10] Cristina Alcaraz, Javier Lopez, Kim-Kwang Raymond Choo, Resilient interconnection in cyber-physical control systems, Computers & Security, Volume 71, November 2017, Pages 2-14. DOI: 10.1016/j.cose.2017.03.004.
[11] Niv Goldenberg, Avishai Wool, Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, International Journal of Critical Infrastructure Protection, Volume 6, Issue 2, June 2013, Pages 63-75. DOI: 10.1016/j.ijcip.2013.05.001.
[12] Rafael Ramos Regis Barbosa, Ramin Sadre, Aiko Pras, Flow whitelisting in SCADA networks, Interna-tional Journal of Critical Infrastructure Protection, Volume 6, Issues 3–4, December 2013, Pages 150-158. DOI: 10.1016/j.ijcip.2013.08.003.
[13] Gritsay, G., Timorin, Yu, Goltsev, A., Positive Technologies. Safety of industrial systems in figures. Access mode: https://www.ptsecurity.com/upload/corporate/ru-en/analytics/SCADA- analytics-eng.pdf. (in Russian).
[14] Mikhailov, D.M., Zhukov, I.Yu., Sheremet, I.A. Zashhita avtomatizirovannyx sistem ot informacionno-texnologicheskix vozdejstvij, NRNU MEPhI, 2014, P.184 (in Russian).
[15] Pischik, B.N. Bezopasnost ASU TP. ZhVT. 2013. No. P.170-175. (in Russian).
[16] Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S., Timorin, A., Industrial control systems and their online availability. Access mode: https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Availability_Statistics.pdf.

Поступила в редакцию – 12 декабря 2017 г. Окончательный вариант –19 февраля 2018 г.
Received – December 12, 2017. The final version – February 19, 2018.