УДК 004.056.5
DOI: 10.17586/0021-3454-2019-62-4-331-339

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Ю. С. Андреев, А. М. Дергачев, Ф. А. Жаров, Д. С. Садырин

Университет ИТМО, 197101, Санкт-Петербург, Россия
E-mail: amd@corp.ifmo.ru

Рассмотрены современные принципы построения автоматических систем управления технологическими процессами (АСУТП), а также их программные и аппаратные компоненты. Проанализированы особенности систем диспетчеризации разных поколений реализации АСУТП. Исследованы угрозы и уязвимости в области информационной безопасности АСУТП. Рассмотрены источники заражения промышленных систем и приведена статистика их использования. Показано, что с ростом вычислительной мощности элементов АСУТП возрастает частота несанкционированного доступа к ним с использованием сети Интернет. Рассмотрен пример новой угрозы безопасности, которую вносит использование протоколов интернета вещей при работе с визуальными данными. Приведены основные меры защиты АСУТП, примеры нормативных документов, регламентирующих действия по обеспечению информационной безопасности и примеры программных и аппаратных продуктов, направленных на их реализацию.

Ключевые слова: *АСУТП, информационная безопасность, программируемые логические контроллеры, ПЛК, SCADA, интернет вещей*

Автоматизированные системы управления технологическими процессами (АСУТП) применяются во многих важных для общества отраслях: машиностроение, приборостроение, транспортные сети [1], электроэнергетика [2], водоснабжение [3], атомная промышленность [4, 5] и др. Сбои в их работе на критически важных объектах могут привести не только к финансовым убыткам, но и к катастрофическим последствиям [6—8]. Меры по обеспечению безопасности критически важных объектов принимаются, в том числе и на законодательном уровне*, однако тема информационной безопасности удостоилась пристального внимания только после инцидента с иранскими ядерными объектами в 2010 г. Этот год стал поворотным в истории киберфизической безопасности вследствие появления первого в истории оружия кибервойны — Stuxnet [9, 10]. В отличие от распространенных на тот момент атак на программное обеспечение Stuxnet была направлена на промышленные контроллеры, которые могут управлять любыми физическими устройствами (такими как насосы, клапаны, электроприводы) или снимать данные с различных датчиков и измерительных приборов, например, тахометров и термометров. Манипуляции с такими контроллерами могут привести не только к нарушению производственных процессов, но и к физическому повреждению оборудования и полному разрушению (уничтожению) критически важных объектов. После этого инцидента количество обнаруженных уязвимостей АСУТП компонентов значительно возросло [11] — с 2010 по 2012 г. было обнаружено в 20 раз больше уязвимостей, чем за предыдущие 5 лет, в том числе уязвимостей N в оборудовании таких известных производителей, как Advantech/Broadwin, GeneralElectric, Siemens, SchneiderElectric, InvensysWonderware. Динамика обнаружения уязвимостей в компонентах АСУТП с 2013 по 2017 год приведена на рис. 1.

* Федеральный закон от 21.11.1995 №170-ФЗ „Об использовании атомной энергии“.

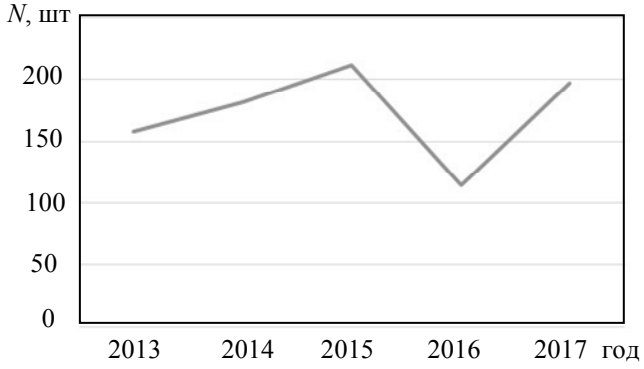

Рис. 1

Подходы к обеспечению информационной безопасности АСУТП отличаются от обеспечения безопасности информационно-вычислительных систем в целом ввиду ряда особенностей их реализации и эксплуатации:

— управление технически сложными жизненно важными объектами;

— работа в режиме реального времени;

— критичность ко времени реакции системы;

— большое время жизненного цикла системы;

— территориальная распределенность;

— отсутствие единой технологии проектирования и модернизации и универсальной элементной базы.

Ранее вероятность таких инцидентов, как заражение программного обеспечения компонентов АСУТП вредоносными программами Stuxnet [10], Duqu [12] или Flame [13], считалась небольшой. Причиной тому были принципы, которые применялись при построении АСУТП: закрытое программное обеспечение, протоколы и технологии [14], физическая изоляция [15]. Данные принципы делали труднодоступной и малоэффективной атаку на автоматизированные системы и промышленные объекты автоматизации.

Однако изменения в аппаратном и программном обеспечении современных АСУТП привели к возникновению новых видов уязвимости, которые не могут быть ликвидированы существующими подходами к обеспечению информационной безопасности. Кроме того, целью атаки на промышленные объекты могут быть не только разрушение, но и политическое давление [10].

Ниже перечислены основные изменения в элементной базе и архитектуре АСУТП, повлекшие появление новых уязвимостей в системе информационной безопасности:

— внедрение открытых сетевых коммуникационных протоколов;

— увеличение мощности вычислительных устройств (примером могут служить программируемые логические контроллеры, ПЛК);

— взаимодействие компонентов распределенных систем через сеть, в том числе Интернет;

— интеграция с корпоративными сетями и информационными системами.

Усложняет задачу обеспечения безопасности в целом то, что изменения могут охватывать не всю систему, а только отдельные ее модули. С одной стороны, облегчает злоумышленникам доступ к АСУТП сетям наличие доступных для публичного просмотра примеров использования существующих уязвимостей. С другой стороны, изменения породили новые способы извлечения выгоды: вымогательство и нецелевое использование вычислительной мощности. Далее рассмотрим примеры изменения элементной базы и архитектуры.

Примером внедрения открытых протоколов и работы через внешнюю сеть могут служить изменения в системах SCADA (Supervisory Control And Data Acquisition, диспетчерское управление и сбор данных): SCADA-системы второго поколения распределенные, но исполь-

зуют нестандартные протоколы связи, третьего поколения — применяют TCP/IP и другие распространенные протоколы [16], четвертого — протоколы интернета вещей. SCADA-системы обеспечивают диспетчерский контроль за удаленными процессами, а в некоторых случаях и управляют ими в случаях неполадок и сбоев. Предоставление доступа к компонентам производственных систем через Интернет как осложняют, так и облегчают эксплуатацию этих систем. Угрозы, характерные ранее для корпоративных сетей, стали актуальными и для сетей АСУТП. Согласно статистике компании Positive tehnologies, в 2017 г. Интернет обеспечивал доступ к 175 632 элементам АСУТП, в основном по протоколу http, на втором и третьем месте — протоколы FOX и Ethernet/IP. Доля доступных SCADA-систем в 2017 г. увеличилась по сравнению с 2016 г. с 13,6 до 14,2 % [17].

Повысить вычислительную мощность позволяют программируемые логические контроллеры, сетевые устройства и полевые элементы контроля и измерения. В середине двадцатого века управление осуществлялось с помощью релейных схем [18]. В 1968 г. создан первый ПЛК [19], термин ПЛК был введен в стандартах EN 61131 (МЭК 61131)[**]. Сейчас ПЛК — это вычислительные устройства, использующие системы реального времени. Стоимость защищенных промышленных операционных систем высока, специализированные системы дешевле, но более открыты для атак. Альтернативой таким ПЛК являются программные продукты, которые могут запускаться на обычных персональных компьютерах [20, 21], однако при этом многократно возрастают риски атак, в частности, через Интернет.

В 2017 г. доля доступных через сеть *d* Интернет ПЛК возросла с 12,9 до 13,2 %, сетевых устройств — с 5,1 до 12,9 %, электроизмерительных приборов — с 5,2 до 6,3 % (рис. 2). Наибольшее количество потенциально уязвимых элементов (26813) выпускает Honeywell. В десятку „уязвимых“ входят такие известные компании, как Lantronix, Simens, Rockwell Automation, Moxa и Schneider Electric. Наибольшее количество элементов АСУТП доступно посредством сети Интернет в США и Германии. В России в 2017 году было доступно 892 элемента, что в 1,5 раза больше, чем в 2016 г. [17].

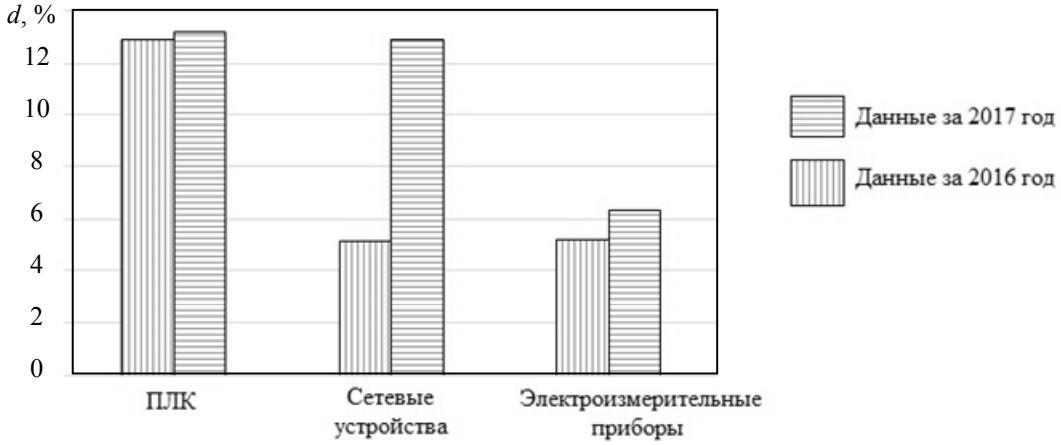

Рис. 2

Увеличение вычислительной мощности элементов промышленных систем и сетей приводит к тому, что АСУТП может подвергаться как вредоносным атакам, так и нецелевому использованию злоумышленниками, в частности, для производства электронных валют. Так, в 2017 г. атакам майнинговых программ подвергалось до 2,1 % элементов, а в первом полугодии 2018 — 6 % [22].

Отдельно нужно отметить еще один тип угроз, возникающих при использовании интернета вещей, — это заражение сетей ip-камер. Видеоданные вполне могут послужить для организации преступлений, не связанных с информационной безопасностью самих АСУТП [22].

[**] ГОСТ Р 51840-2001 (МЭК 61131-1-92). Программируемые контроллеры. Общие положения и функциональные характеристики. Введ. 01.01.2003. М.: Изд-во стандартов, 2002.

Из-за перехода на стандартные сетевые протоколы взаимодействия компонентов АСУТП возросло и количество случайных заражений промышленных сетей от обычного вредоносного программного обеспечения, основными объектами атак которого в 2017—2018 г. стали: операционная система Windows, программы на языке Visual Basic, программное обеспечение MS Office [22]. Согласно статистике, доля атак через сеть Интернет на системы и компоненты АСУ в 2018 г. возросла в сравнении с 2017 г. с 20,6 до 27,3 %, при этом доля атак через съемные носители уменьшилась с 9,3 до 8,4 %, а через почтовые клиенты — с 3,9 до 3,8 % [22]. В целом с 2017 по 2018 г. доля компонентов АСУТП, подвергшихся атакам, достигла 41,2 %. Некоторые исследователи связывают географию распространения атак на эти системы с уровнем экономического развития стран и регионов мира [22].

Ранее для разработки таких вредоносных программ, как Stunex, требовались большие материальные затраты, осведомленность в принципе работы системы, доступ к оборудованию. Теперь доступ к элементам промышленной системы и стандартные принципы их взаимодействия через сеть облегчают создание и применение вредоносного программного обеспечения, рассчитанного как на кратковременное, так и на длительное использование для нанесения ущерба в промышленном масштабе. Примером могут служить выявленные в 2017 г. такие вредоносные программы, как Shamoon 2.0/StoneDrill [23] и CrashOverride/Industroyer [24] (последняя программа может быть отнесена к кибероружию). Эксперты „Лаборатория Касперского“ фиксировали и ранее рост интереса злоумышленников к промышленным компаниям и организациям [26].

Важное место в обеспечении информационной безопасности как разрабатываемых, так и эксплуатируемых АСУТП занимают инструментальные средства, предназначенные для выявления атак [26—28] на основе баз знаний уязвимостей, разработанных и собранных различными государствами и компаниями [31]. Утечки „штаммов“ вредоносного программного обеспечения в виде коллекции вредоносных программ нередко становятся товаром на рынке киберпреступности и представляют вторичную угрозу безопасности АСУТП. Таким образом, например, особое распространение получили атаки программ-шифровальщиков. В целом в 63 странах было обнаружено 33 семейства данного вида программ, среди которых самыми известными стали WannaCry [29] и ExPetr [30].

Меры обеспечения информационной безопасности АСУТП можно разделить на административные и программно-технические. Первые направлены на разработку регламентирующих документов, методы обеспечения информационной безопасности АСУТП. Следует отметить, что данные меры могут различаться для разных стран, компаний и отраслей. Примерами общих стандартов могут служить ISA/IEC 62443[*], документы КСИИ[**], приказ ФСТЭК 31[***]; отраслевых: NERC CIP — стандарт защиты инфраструктуры передачи электроэнергии [32], Guidance for Addressing Cyber Security in the Chemical Industry — группа стандартов защиты химических производств [33].

Программно-технические меры обеспечивают основную часть информационной безопасности АСУТП [34]:

— управление доступом: комплекс аппаратной загрузки „Тверца“ и его модификации, аппаратный замок „Соболь“ [35], программно-аппаратный комплекс „Блокхост-МДЗ“, систе-

[*] ISA/IEC 62443 „Security for Industrial Automation and Control Systems“. 2018.

[**] Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры ФСТЭК России утв. 18.05.2007. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры ФСТЭК России утв. 18.05.2007. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры ФСТЭК России утв. 19.11.2007.

[***] Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31. Введ. 17.08.2014.

ма управления доступом ОС QNX [36], программный комплекс „СТРАЖ-ЧПУ“, многофункциональное устройство АПК „ЩИТ“ и пр.;

— обеспечение целостности: комплекс „Тверца“, индустриальный криптографический модуль ViPNet ICM;

— обеспечение безопасного межсетевого взаимодействия: средство криптографической защиты информации АПК „Свиток“, анализатор сетевого трафика Kaspersky TMS;

— обеспечение антивирусной защиты: Kaspersky Industrial CyberSecurity [37], антивирус ПК АВЗ КПДА.94201-01 [38];

— анализ защищенности: средство анализа защищенности „Сканер-ВС“, Kaspersky System Manager и пр.;

— обнаружение вторжений: межсетевой экран и система обнаружения вторжений „Рубикон“, шлюз безопасности Ideco ICS [39] и пр.;

— управление системой: ОС Kaspersky [40], ОС QNX, ОС Neutrino, Astra Linux [41] и многие другие.

Следует отметить, что многие фирмы предлагают готовые решения для всех уровней АСУТП: ЗОСРВ „Нейтрино“, семейство программных продуктов для автоматизации от Kaspersky, CISCO [42] и многие другие. Такие решения хорошо подходят для масштабных проектов, но слишком дороги для небольших производств.

Главными характеристиками АСУТП являются время и корректность реакции системы [43]. Вторжение в систему приводит к изменению этих показателей, что является маркером злонамеренных действий. Однако мониторинг таких показателей систем используется лишь как элемент оповещения о чрезвычайной ситуации.

Несмотря на все многообразие мер защиты и руководящих принципов информационная безопасность АСУТП остается актуальной темой и требует больших затрат для поддержания должного уровня защиты и отражения новых угроз. Решением проблемы могла бы стать интегрированная в АСУТП система мониторинга на основе эталонной поведенческой модели.

СПИСОК ЛИТЕРАТУРЫ

1. *Безродный К. П., Культин И. В., Лебедев М. О.* Автоматизированная система управления технологическими процессами (АСУ ТП) в железнодорожных тоннелях Олимпийской трассы // Транспорт Российской Федерации. Журнал о науке, практике, экономике. 2009. № S. С. 24—26.

2. *Рогов С. Л.* Распределенные системы АСУ ТП в энергетике — мода или необходимость. Ч. 1 // ИСУП. 2008. № 2. С. 15—21.

3. *Зуев К. И.* Автоматизация систем водоснабжения и водоотведения. Владимир: Изд-во ВлГУ, 2016. 224 с.

4. *Бывайков М. Е., Жарко Е. Ф., Менгазетдинов Н. Э.* и др. Опыт проектирования и внедрения системы верхнего блочного уровня АСУТП АЭС // Автоматика и телемеханика. 2006. № 5. С. 65—68.

5. *Менгазетдинов Н. Э., Полетыкин А. Г., Промыслов В. Г., Зуенкова И. Н., Бывайков М. Е., Прокофьев В. Н., Коган И. Р., Коршунов А. С., Фельдман М. Е., Кольцов В. А.* Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУТП для АЭС „Бушер“ на основе отечественных информационных технологий. М.: ИПУ РАН, 2013. 95 с.

6. Bundesamt für Sicherheit in der Informationstechnik. Druck- und Verlagshaus Zarbock Frankfurt am Main 2014. Die Lage der IT-Sicherheit in Deutschland. 2014. S. 31.

7. Отдел исследования киберугроз CyS Centrum. Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины [Электронный ресурс]: <https://cys-centrum.com/ru/news/black_energy_2_3>. (дата обращения 25.01.2019).

8. *Михайлов Д. М., Жуков И. Ю., Шеремет И. А.* Защита автоматизированных систем от информационно-технологических воздействий. М.: НИЯУ МИФИ, 2014. 184 с.

9. *Langner R.* Stuxnet: Dissecting a cyberwarfare weapon // IEEE Security & Privacy. 2011. Vol. 9, N 3. P. 49—51.

10. *Арефьев А. С.* Таргетированные атаки на промышленный сектор: новое оружие в кибервойне // Автоматизация в промышленности. 2015. № 2. С. 43—45.

11. *Пищик Б. Н.* Безопасность АСУ ТП // Вычислительные технологии. 2013. Т. 18. С. 170—175.

12. Symantec Security Response. W32.Duqu: The Precursor to the Next Stuxnet [Электронный ресурс]: <http://www.symantec.com/ru/ru/outbreak/?id=stuxnet>. (дата обращения 27.01.2019).

13. *Gostev A.* The Flame: Questions and Answers. SECURELIST [Электронный ресурс]: <http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers>. (дата обращения 05.02.2019).

14. *Colbert E. J. M., Kott A.* Cyber-security of SCADA and Other Industrial Control Systems. Springer International Publishing Switzerland, 2016. P. 7.

15. Эволюция индустриальной кибербезопасности. Построение интеллектуальных систем обеспечения защиты АСУ ТП промышленных предприятий // Information Security/Информационная безопасность. 2016. № 1. С. 17.

16. *Поляков В. А.* Удаленный мониторинг и управление в Интернете вещей: AggreGate SCADA/HMI // ИСУП. 2015. № 5. С. 59.

17. Positive Technologies. Безопасность АСУ-ТП: итоги 2017 года [Электронный ресурс]: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-2017-rus.pdf>. (дата обращения 08.02.2019).

18. *Смородин Г. С., Лысенко В. С., Манежнов В. Г.* Развитие релейной техники в России // Молодой ученый. 2016. № 29. С. 138—140.

19. Борьба за разработку ПЛК: взгляд изнутри // Control Engineering Россия. 2014. Т. 54, № 6. С. 79—81.

20. *Бычков И. Н., Глухов В. И., Трушкин К. А.* Доверенная программно-аппаратная платформа „Эльбрус“. Отечественное решение для АСУ ТП КВО // ИСУП. 2014. № 1. С. 49.

21. *Золоторев С. В.* Технология программирования контроллеров ISaGRAF 6: превращение в Единую Платформу Автоматизации // ИСУП. 2011. № 2. С. 32.

22. Лаборатория Касперского. Ландшафт угроз для систем промышленной автоматизации: первое полугодие 2018 [Электронный ресурс]: <https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/#_Toc523499582>. (дата обращения 09.02.2019).

23. От Shamoon к StoneDrill Wiper-подобные программы атакуют компании в Саудовской Аравии и не только [Электронный ресурс]: <https://securelist.ru/from-shamoon-to-stonedrill/30350/>. (дата обращения 09.02.2019).

24. CRASHOVERRIDE Analyzing the Threat to Electric Grid Operations [Электронный ресурс]: <https://dragos.com/wp-content/uploads/CrashOverride-01.pdf>. (дата обращения 10.02.2019).

25. Лаборатория Касперского. Ландшафт угроз в 2017 году [Электронный ресурс]: <https://ics-cert.kaspersky.ru/reports/2017/11/30/industrial-enterprise-and-iot-security-threats-forecast-for-2018/>. (дата обращения 11.02.2019).

26. *Maynor D.* Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research. Syngress, 2007. 350 p.

27. *Bodenheim R., Butts J., Dunlap S., Mullins B. E.* Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices // Intern. J. of Critical Infrastructure Protection. 2014. Vol. 7, Is. 2, June. P. 114—123.

28. Thingful Blog [Электронный ресурс]: <http://thingful/>. (дата обращения 11.02.2019).

29. *Бигаева Д. Б., Бигаев А. Б.* Система информационной безопасности российской федерации // Вестник науки и образования. 2017. № 7. С. 31.

30. *Нестеренко Е. А., Козлова А. С.* Направления развития цифровой экономики и цифровых технологий в России // ИБР. 2018. № 2. С. 31.

31. *Гостев А. А.* Kaspersky security bulletin 2012. Кибероружие // Право и кибербезопасность.2012. № 1. С. 66—71.

32. NERC Roster. North American Electric Reliability Corporation. 9 October 2015. P. 44—65.

33. Guidance for Addressing Cyber Security in the Chemical Industry, Version 3.0. ACC ChemITC Chemical Sector Cyber Security Program, May 2006.

34. *Надеждин Ю. М.* Безопасность АСУ ТП критически важных объектов // Системы безопасности. 2014. № 2. С. 40.

35. *Зайцев А. С.* Защита информации ограниченного доступа в учреждении социального обеспечения // Гаудеамус. 2014. № 2. С. 24.

36. Перспективы встраиваемых технологий QNX: технологии будущего для реального времени (Пресс-релиз) // Прикладная информатика. 2010. № 3. С. 3—4.

37. Кибербезопасность промышленных систем. Практикум по программе „Лаборатории Касперского“. Обучить самое уязвимое // ИСУП. 2018. № 1. С. 73.

38. Антивирусная защита ПК АВЗ КПДА.94201-01 [Электронный ресурс]: <http://www.kpda.ru/products/antivirus>. (дата обращения 12.02.2019)

39. *Чемодуров А. С., Карпутина А. Ю.* Обзор средств фильтрации трафика в корпоративной сети // Концепт. 2015. № 2. С. 71—75 [Электронный ресурс]: <http://e-koncept.ru/2015/15039.htm>.

40. Настало время безусловной безопасности: операционная система «Лаборатории Касперского» выходит на рынок [Электронный ресурс]: <http://www.kaspersky.ru/about/news/business/2016/KasperskyOS/>. (дата обращения 12.02.2019)

41. *Буренин П. В., Девянин П. Н., Лебеденко Е. В.* и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. М.: Горячая линия — Телеком, 2016. 312 с.

42. Решения Cisco по защите автоматизированных систем управления технологическими процессами [Электронный ресурс]: <https://www.cisco.com/assets/global/RU/pdfs/brochures/Podhod-Cisco-po-bezopasnosti-ASU-TP.pdf>. (дата обращения 12.02.2019)

43. *Дроботун Е. Б.* Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. СПб: Наукоемкие технологии, 2017. 120 с.

Сведения об авторах

Юрий Сергеевич Андреев — канд. техн. наук; Университет ИТМО; факультет систем управления и робототехники; E-mail: ysandreev@corp.ifmo.ru

Андрей Михайлович Дергачев — канд. техн. наук; Университет ИТМО; факультет программной инженерии и компьютерной техники; E-mail: amd@corp.ifmo.ru

Федор Андреевич Жаров — аспирант; Университет ИТМО; факультет программной инженерии и компьютерной техники; E-mail: zhar.feda@yandex.ru

Даниил Сергеевич Садырин — аспирант; Университет ИТМО; факультет программной инженерии и компьютерной техники; E-mail: dssadyrin@corp.ifmo.ru

Поступила в редакцию
13.02.19 г.

Ссылка для цитирования: *Андреев Ю. С., Дергачев А. М., Жаров Ф. А., Садырин Д. С.* Информационная безопасность автоматизированных систем управления технологическими процессами // Изв. вузов. Приборостроение. 2019. Т. 62, № 4. С. 331—339.

INFORMATION SECURITY OF AUTOMATED CONTROL SYSTEMS OF TECHNOLOGICAL PROCESSES

Yu. S. Andreev, A. M. Dergachev, F. A. Zharov, D. S. Sadyrin

ITMO University, 197101, St. Petersburg, Russia
E-mail: amd@corp.ifmo.ru

The modern principles of automatic process control systems (ACS-TP) design are considered, as well as the systems software and hardware components. Specific features of dispatch system characteristics of different generations of the ACS-TP implementation are analyzed. A review of existing threats and vulnerabilities in the field of information security of ACS-TP is presented. It is shown that the recent increase in computing power of ACS-TP elements is accompanied by an increase in unauthorized access to them using the Internet. A new security threat introduced by implementation of the Internet of Things pro-

tocols when working with visual data is described. A classification of the main measures aimed at protecting the automated process control systems is given, examples of regulatory documents governing actions to ensure information security and examples of software and hardware products aimed at their implementation are presented.

Keywords: ACS-TP, information security, programmable logic controller, PLC, SCADA, internet of things

REFERENCES

1. Bezrodnyy K.P., Kul'tin I.V., Lebedev M.O. *Transport Rossiyskoy Federatsii*, 2009, no. S, pp. 24–26. (in Russ.)
2. Rogov S.L. *Informatizatsiya i Sistemy Upravleniya v Promyshlennosti*, 2008, no. 2, pp. 15–21. (in Russ.)
3. Zuyev K.I. *Avtomatizatsiya sistem vodosnabzheniya i vodootvedeniya* (Automation of Water Supply and Drainage Systems), Vladimir, 2016, 224 p. (in Russ.)
4. Byvaikov M.E., Zharko E.F., Mengazetdinov N.E., Poletykin A.G., Prangishvili I.V., Promyslov V.G. *Automation and Remote Control*, 2006, no. 5(67), pp. 735–747.
5. Mengazetdinov N.E., Poletykin A.G., Promyslov V.G., Zuyenkova I.N., Byvaykov M.E., Prokof'yev V.N., Kogan I.R., Korshunov A.S., Fel'dman M.E., Kol'tsov V.A. *Kompleks rabot po sozdaniyu pervoy upravlyayushchey sistemy verkhnego blochnogo urovnya ASUTP dlya AES "Busher" na osnove otechestvennykh informatsionnykh tekhnologiy* (The Complex of Works on the Creation of the First Control System of the Upper Block Level of the Automated Process Control System for Bushehr NPP Based on Domestic Information Technologies), Moscow, 2013, 95 p. (in Russ.)
6. *Bundesamt für Sicherheit in der Informationstechnik*, Druck- und Verlagshaus Zarbock Frankfurt am Main 2014, Die Lage der IT-Sicherheit in Deutschland, 2014, S. 31.
7. https://cys-centrum.com/ru/news/black_energy_2_3. (in Russ.)
8. Mikhaylov D.M., Zhukov I.Yu., Sheremet I.A. *Zashchita avtomatizirovannykh sistem ot informatsionno-tekhnologicheskikh vozdeystviy* (Protection of Automated Systems from Information Technology Impacts), Moscow, 2014, 184 p. (in Russ.)
9. Langner R. *IEEE Security & Privacy*, 2011, no. 3(9), pp. 49–51.
10. Aref'yev A. S. *Automation in Industry*, 2015, no. 2, pp. 43–45. (in Russ.)
11. Pishchik B.N. *Computational Technologies*, 2013, no. 18, pp. 170–175. (in Russ.)
12. *Symantec Security Response. W32.Duqu: The Precursor to the Next Stuxnet*, http://www.symantec.com/ru/ru/outbreak/?id=stuxnet.
13. Gostev A. *The Flame: Questions and Answers. SECURELIST*, http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers.
14. Colbert E.J.M., Kott A. *Cyber-security of SCADA and Other Industrial Control Systems*, Springer International Publishing Switzerland, 2016, pp. 7.
15. *Evolyutsiya industrial'noy kiberbezopasnosti. Postroyeniye intellektual'nykh sistem obespecheniya zashchity ASU TP promyshlennykh predpriyatiy* (The Evolution of Industrial Cybersecurity. Construction of Intelligent Systems to Ensure the Protection of Industrial Process Control Systems), Information Security, 2016, no. 1, pp. 17. (in Russ.)
16. Polyakov V.A. *Informatizatsiya i Sistemy Upravleniya v Promyshlennosti*, 2015, no. 5, pp. 59. (in Russ.)
17. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-2017-rus.pdf. (in Russ.)
18. Smorodin G.S., Lysenko V.S., Manezhnov V.G. *Molodoy uchenyy*, 2016, no. 29, pp. 138–140. (in Russ.)
19. *Bor'ba za razrabotku PLK: vzglyad iznutri* (Fight for PLC Development: an Inside View), Control Engineering Rossiya, 2014, no. 6(54), pp. 79–81. (in Russ.)
20. Bychkov I.N., Glukhov V.I., Trushkin K.A. *Informatizatsiya i Sistemy Upravleniya v Promyshlennosti*, 2014, no. 1, pp. 49. (in Russ.)
21. Zolotorev S.V. *Informatizatsiya i Sistemy Upravleniya v Promyshlennosti*, 2011, no. 2, pp. 32.
22. https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/#_Toc523499582. (in Russ.)
23. https://securelist.ru/from-shamoon-to-stonedrill/30350/. (in Russ.)
24. *CRASHOVERRIDE Analyzing the Threat to Electric Grid Operations*, https://dragos.com/wp-content/uploads/CrashOverride-01.pdf.
25. https://ics-cert.kaspersky.ru/reports/2017/11/30/industrial-enterprise-and-iot-security-threats-forecast-for-2018/. (in Russ.)
26. Maynor D. *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research*, Syngress, 2007, 350 p.
27. Bodenheim R., Butts J., Dunlap S., Mullins B.E. *Intern. J. of Critical Infrastructure Protection*, 2014, no. 2(7), June, pp. 114–123.
28. Thingful Blog, http://thingful/.
29. Bigayeva D.B., Bigayev A.B. *Herald of Science and Education*, 2017, no. 7, pp. 31. (in Russ.)
30. Nesterenko E.A., Kozlova A.S. *Ekonomicheskaya bezopasnost'' i kachestvo*, 2018, no. 2, pp. 9–14. (in Russ.)
31. Gostev A.A. *Law and Cyber Security* (Legal Issues of Communication), 2012, no. 1, pp. 66–71. (in Russ.)

32. *NERC Roster. North American Electric Reliability Corporation*. 9 October 2015. pp. 44–65.
33. *Guidance for Addressing Cyber Security in the Chemical Industry*, Version 3.0. ACC ChemITC Chemical Sector Cyber Security Program, May 2006.
34. Nadezhdin Yu.M. *Security and safety*, 2014, no. 2, pp. 40. (in Russ.)
35. Zaytsev A.S. *Gaudeamus*, 2014, no. 2, pp. 24. (in Russ.)
36. *Perspektivy vstraivayemykh tekhnologiy QNX: tekhnologii budushchego dlya real'nogo vremeni (Press-reliz)* (QNX Embedded Technology Perspectives: Real-Time Future Technologies (Press Release)), Journal of Applied Informatics, 2010, no. 3, pp. 3–4. (in Russ.)
37. *Kiberbezopasnost' promyshlennykh sistem. Praktikum po programme "Laboratorii Kasperskogo". Obuchit' samoye uyazvimoye* (Cybersecurity Industrial Systems. Workshop on the Program "Kaspersky Lab." Train the Most Vulnerable), Informatizatsiya i Sistemy Upravleniya v Promyshlennosti, 2018, no. 1, pp. 73. (in Russ.)
38. http://www.kpda.ru/products/antivirus. (in Russ.)
39. Chemodurov A.S., Karputina A.Yu. *Koncept*, 2015, no. 2, pp. 71–75, http://e-koncept.ru/2015/15039.htm. (in Russ.)
40. http://www.kaspersky.ru/about/news/business/2016/KasperskyOS/. (in Russ.)
41. Burenin P.V., Devyanin P.N., Lebedenko E.V. et al. *Bezopasnost' operatsionnoy sistemy spetsial'nogo naznacheniya Astra Linux Special* (Edition Security of the Special-Purpose Operating System Astra Linux Special Edition), Moscow, 2016, 312 p. (in Russ.)
42. https://www.cisco.com/assets/global/RU/pdfs/brochures/Podhod-Cisco-po-bezopasnosti-ASU-TP.pdf.
43. Drobotun E.B. *Teoreticheskiye osnovy postroyeniya sistem zashchity ot komp'yuternykh atak dlya avtomatizirovannykh sistem upravleniya* (Theoretical Foundations of Building Systems for Protection against Computer Attacks for Automated Control Systems), St. Petersburg, 2017, 120 p. (in Russ.)

Data on authors

Yury S. Andreev	—	PhD; ITMO University, Faculty of Control Systems and Robotics; E-mail: ysandreev@corp.ifmo.ru
Andrey M. Dergachev	—	PhD; ITMO University, Faculty of Software Engineering and Computer Systems; E-mail: amd@corp.ifmo.ru
Fedor A. Zharov	—	Post-Graduate Student; ITMO University, Faculty of Software Engineering and Computer Systems; E-mail: zhar.feda@yandex.ru
Daniil S. Sadyrin	—	Post-Graduate Student; ITMO University, Faculty of Software Engineering and Computer Systems; E-mail: dssadyrin@corp.ifmo.ru

For citation: Andreev Yu. S., Dergachev A. M., Zharov F. A., Sadyrin D. S. Information security of automated control systems of technological processes. *Journal of Instrument Engineering*. 2019. Vol. 62, N 4. P. 331—339 (in Russian).

DOI: 10.17586/0021-3454-2019-62-4-331-339