DOI: 10.51790/2712-9942-2021-2-4-6

О НЕОБХОДИМОСТИ СОЗДАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СРЕДСТВ УПРАВЛЕНИЯ СИСТЕМАМИ С КРИТИЧЕСКОЙ МИССИЕЙ

В. Б. Бетелин[1], **Д. А. Моргун**[2]

[1] *Федеральное государственное учреждение «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук», г. Москва, Российская Федерация, ORCID: http://orcid.org/0000-0001-6646-2660, betelin@inbox.ru*

[2] *Сургутский филиал Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук», г. Сургут, Российская Федерация, ORCID: https://orcid.org/0000-0003-0692-1583, morgun_da@office.niisi.tech*

Аннотация: происходящие в мире события свидетельствуют о возрастании угрозы перехвата управления системами с критической миссией (СКМ). Приводятся конкретные примеры инцидентов, один из них — массовые отключения электроэнергии в Венесуэле. Обосновывается необходимость разработки технологии создания цифровых систем управления, обеспечивающей парирование угрозы перехвата управления и нештатного функционирования систем с критической миссией. В основе этой технологии — концепция цифровых двойников объектов управления цифровых систем управления этими объектами, включая все аппаратные и программные компоненты, а также интеллектуальные средства самоконтроля и самокоррекции функционирования элементной базы, вычислительной и коммуникационной техники, базового и прикладного программного обеспечения.

Ключевые слова: системы с критической миссией, цифровые двойники, интеллектуальные средства управления.

Для цитирования: Бетелин В. Б., Моргун Д. А. О необходимости создания интеллектуальных средств управления системами с критической миссией. *Успехи кибернетики*. 2021;2(4):60–66. DOI: 10.51790/2712-9942-2021-2-4-6.

ON THE NEED TO CREATE INTELLIGENT CONTROL SYSTEMS FOR SYSTEMS WITH A CRITICAL MISSION

V. B. Betelin[1], **D. A. Morgun**[2]

[1] *Federal State Institution "Scientific Research Institute for System Analysis of the Russian Academy of Sciences", Moscow, Russian Federation, ORCID: http://orcid.org/0000-0001-6646-2660, betelin@inbox.ru*

[2] *Surgut Branch of Federal State Institute "Scientific Research Institute for System Analysis of the Russian Academy of Sciences", Surgut, Russian Federation, ORCID: https://orcid.org/0000-0003-0692-1583, morgun_da@office.niisi.tech*

Abstract: there is an ongoing threat of control interception in mission-critical systems (MCS). Specific examples of such incidents are presented, one of them is the massive power outages in Venezuela. We specify the reasons for creating an approach to developing digital control systems for MCS resistant to control interception and abnormal functioning. This technology is based on the digital twin concept. A twin represents all the hardware and software components, as includes smart tools for the hardware, core and application software self-monitoring and self-correction.

Keywords: mission-critical systems, trusted systems.

Cite this article: Betelin V. B., Morgun D. A. On the Need to Create Intelligent Control Systems for Systems with a Critical Mission. *Russian Journal of Cybernetics*. 2021;2(4):60–66. DOI: 10.51790/2712-9942-2021-2-4-6.

WannaCry — шифровальщик-вымогатель

12 мая 2017 года начал свое молниеносное распространение по миру сетевой червь WannaCry. На 13 мая было инфицировано 131 233 компьютера [1], на 27 мая — 424 289 компьютеров [2]. . . На 25 мая 2017 года общий ущерб от WannaCry оценивался в 1 млрд долларов США [3].

Сетевой червь WannaCry можно условно охарактеризовать как «бытовой». Он способен нанести вред любому уязвимому компьютеру и не нацелен на какой-то конкретный экземпляр.

Для заражения компьютеров WannaCry использует уязвимость операционных систем Windows. Хакерской группировкой Equation Group, связанной с АНБ, были созданы эксплойт[1] EternalBlue и бэкдор[2] DoublePulsar, позволяющие использовать данную уязвимость для заражения компьютера и получения доступа к нему.

Вредоносная программа сканирует диапазон IP-адресов локальной сети и случайно выбранные IP-адреса сети Интернет в поисках компьютеров с открытым TCP-портом 445, который отвечает за обслуживание протокола SMBv1. Обнаружив такой компьютер, программа предпринимает несколько попыток проэксплуатировать на нем уязвимость EternalBlue и в случае успеха устанавливает бэкдор DoublePulsar, через который загружается и запускается исполняемый код программы WannaCry.

При каждой попытке эксплуатации вредоносная программа проверяет наличие на целевом компьютере DoublePulsar и в случае обнаружения загружается непосредственно через этот бэкдор.

Высокая скорость распространения WannaCry, уникальная для программы-вымогателя, обеспечивается использованием опубликованной в феврале 2017 года уязвимости сетевого протокола SMB операционной системы Microsoft Windows, описанной в бюллетене MS17-010. Компанией-разработчиком подтверждено наличие уязвимости абсолютно во всех пользовательских и серверных продуктах, имеющих реализацию протокола SMBv1 — начиная с Windows XP/Windows Server 2003 и заканчивая Windows 10/Windows Server 2016.

В коде ранних версий программы был предусмотрен механизм самоуничтожения, так называемый Kill Switch: программа проверяла доступность двух определенных Интернет-доменов и в случае их наличия полностью удалялась из компьютера. Такой механизм, однако, не спасает от поражения компьютеры, доступ в Интернет которых подвергается жесткой фильтрации (как, например, в некоторых корпоративных сетях). WannaCry в таком случае не находит Kill Switch, заблокированный политикой Интернет-доступа, и продолжает свое вредоносное действие.

Stuxnet — перехват управления АСУ ТП

Stuxnet — это компьютерный червь, перехватывающий и модифицирующий информационный поток между программируемыми логическими контроллерами марки Simatic S7 и рабочими станциями SCADA системы Simatic WinCC фирмы Siemens. **Уникальность программы заключалась в том, что впервые в истории кибератак вирус физически разрушал инфраструктуру**.

Данный вирус использует четыре уязвимости системы Microsoft Windows (уязвимость «нулевого дня» (zero-day[3]) и три ранее известные уязвимости), позволяющие ему распространяться при помощи USB-flash-накопителей. Оставаться не замеченным антивирусными программами ему помогало наличие настоящих цифровых подписей (два действительных сертификата, выпущенных компаниями Realtek и JMicron).

Бывший аналитик ЦРУ Мэтью Барроуз в книге «Будущее: рассекречено. Каким будет мир в 2030 году» пишет, что червь Stuxnet «смог, пусть и на короткое время, приостановить иранскую ядерную программу. Он нарушил работу почти 1000 центрифуг для обогащения уранового топлива. По мнению экспертов, иранцы, обнаружив вирус и избавившись от 1000 зараженных устройств, смогли предотвратить больший ущерб» [5].

Приведем здесь также слова Роула Шоуэнберга, ведущего антивирусного эксперта североамериканского подразделения «Лаборатории Касперского»: «Но в целом интеллектуальный труд, продуктом которого стал Stuxnet, не менее удивителен и примечателен. Четыре 0-day уязвимости, два краденых цифровых сертификата, прекрасное знание систем SCADA — все было тщательно спланировано и приведено в исполнение» [6].

Stuxnet предполагалось внедрить на компьютеры иранских заводов по обогащению урана. Код программы помогал нарушить штатный режим работы центрифуг Siemens P-1, так что со временем

[1] «Эксплойт» — программа или код, фрагмент кода программы, который использует недостатки в системе безопасности конкретного приложения для заражения устройства [4].

[2] Вредоносная программа для получения доступа к рабочей станции, серверу, устройству или сети путем обхода аутентификации, а также других стандартных методов и технологий безопасности [4].

[3] Уязвимость, о которой еще не знает разработчик (и, соответственно, не существует патчей, ее устраняющих).

центрифуги выходили из строя по «непонятным» причинам. Программа успешно выполнила поставленную задачу. Но проблема в том, что на определенном этапе Stuxnet вышел из под контроля и начал распространяться в Интернете, угрожая другим целям, кроме иранских. Пулитцеровский лауреат Дэвид Сангер в своей книге “Confront and Conceal” говорит, что ошибка была во второй версии программы, которую независимо от американцев написали израильские коллеги.

Новые подробности о последствиях операции «Олимпийские игры» сообщил российский эксперт Евгений Касперский. Во время пресс-конференции в Австралии он сказал, что его друг, который работает на одной из АЭС, обнаружил вирус Stuxnet в локальной сети предприятия, не подключенной к Интернету.

Рассматривая историю создания Stuxnet и последствия его применения, мы видим уже не просто вредоносную программу, а **точно нацеленное «кибероружие» для перехвата управления определенным объектом**.


Бизнес, 15 окт, 19:23 | 444 153 | Поделиться

«Газпрому» принудительно отключили импортную технику через спутник

В «Газпроме» заявили, что австрийские компрессоры отключили дистанционно и они до сих пор не работают. Компания планирует закупить компрессоры российского производства на замену зарубежным

Фото: Виталий Тимкив / ТАСС

Рис. 1. *15 октября 2019 года. «Газпрому» принудительно отключили импортную технику через спутник [7]*

«Дистанционное отключение» продолжается

Вредоносные программы WannaCry и Stuxnet к настоящему времени достаточно хорошо изучены специалистами и освещены в печати. Здесь они приведены в качестве примеров эксплуатации злоумышленниками уязвимостей, имеющихся в компьютерных системах и реализации угроз различного характера. Как показывают оба приведенных примера, вредоносные программы могут наносить ущерб, ощутимый в масштабах государства или даже в мировом масштабе, а в качестве злоумышленников могут выступать, в том числе, спецслужбы государств.

Более свежий пример — Венесуэла: вечером 7 марта 2019 года Каракас и большинство штатов Венесуэлы остались без света. Президент страны Николас Мадуро назвал блэкаут «Электрической войной» со стороны Вашингтона. Отключение произошло в результате хакерской атаки на автоматическую систему управления гидроэлектростанции Гури. Как отметила официальный представитель МИД России Мария Захарова, «Организаторы этой атаки были хорошо знакомы с устройством оборудования. Речь идет о комплексном воздействии на систему управления и контроля основных электрораспределительных станций» [8].

Отметим, что в качестве уязвимости промышленного оборудования, несущей в себе угрозу остановки технологического или производственного процесса, можно рассматривать сам факт наличия возможности у зарубежного производителя дистанционного управления оборудованием клиента.

При том, что дистанционное отключение оборудования клиентов несет репутационные риски для производителей оборудования, оно вполне применяется в рамках санкционной политики (рис. 1).

Недокументированные возможности как уязвимости

В настоящее время каждый процессор компании Intel снабжен штатно неотключаемой аппаратно-программной компонентой Intel Management Engine (ME). Данная компонента может располагаться в отдельной СБИС, внутри контроллера Ethernet, внутри системного контроллера (northbridge) или внутри СнК, на котором процессорные ядра и системный контроллер интегрированы в одну СБИС. Данная компонента имеет наивысшие привилегии, допускающие неограниченный доступ компоненты ко всем аппаратным ресурсам.

Одновременно, сама компонента оказывается аппаратно защищена от любого доступа со стороны ядра операционной системы или даже гипервизора.

У компании AMD, начиная с 2013 года, также есть подобная компонента, называемая Platform Security Processor.

Современные СнК[4] архитектуры ARM имеют в своем составе основной набор ядер, функционирующий под управлением операционной системы (Android или iOS), и вспомогательные ядра, на которых реализуются функции радиомодема для доступа к мобильным (сотовым) сетям и функции обеспечения безопасности: проверка цифровых подписей загрузчика, ядра ОС, хранение ключей шифрования и пр.

Как свидетельствуют результаты современных исследований, производители оборудования, системного и прикладного программного обеспечения ведут активный сбор сведений [9]:

- практически в каждом современном программном или аппаратном продукте имеется функция слежения и отправки статистики, как правило, включенная по умолчанию. Например, компонента драйвера NVIDIA — NVIDIA Telemetry Container, драйверы Intel и др.;
- информация о корпоративных сетях наших учреждений, предприятий и организаций и персональная информация о наших сотрудниках в реальном времени, на законном основании или скрытно собирается и обрабатывается в основном за пределами РФ в компаниях, находящихся в большинстве своем под юрисдикцией одной страны — США;
- по данным компании POSITIVE TECHNOLOGIES (второй квартал 2020 года), над массовыми атаками преобладают целенаправленные атаки (63 %). Наибольший интерес представляют государственные учреждения, промышленные компании, финансовый сектор и сфера науки и образования [10].

Мы не всегда можем определить, чем занимается наш компьютер

Приведем некоторые результаты эксперимента по косвенному мониторингу несанкционированной активности в вычислительных системах [11].

В настоящий момент авторами [11] ведется обработка статистических данных, полученных при эксплуатации более 100 однородных компьютеров с фиксацией более 100 различных параметром работы компьютеров. Компьютеры эксплуатируются в высшем учебном заведении и задействованы в учебном процессе. Основное время мониторинга — с 22:00 до 7:00 утра следующего дня. Выбрано время мониторинга, когда активных действий пользователи не осуществляют. При этом выполняется проверка показателей потребления электроэнергии и нагрузки на ЦП.

Выявлены некоторые аномалии поведения компьютеров. Например, ниже представлен один из встречающихся вариантов поведения. Аномалия поведения заключается в следующем.

Температурная нагрузка на ядра процессора в норме сохранятся примерно до часа ночи (в других подобных случаях $\pm$ 2 часа).

После часа ночи наблюдаются множественные температурные всплески от 32° С до 48° С (система охлаждения работает нормально), рост энергопотребления центральным процессором и отдельными ядрами.

В дневное время, когда на компьютерах работают студенты, всё функционирует в штатном режиме. Дополнительно проверялись планировщики задач, работа антивирусов, сетевой карты, и существенных признаков их активности не наблюдалось. При этом роста энергопотребления оперативной

[4] Системы на кристалле.

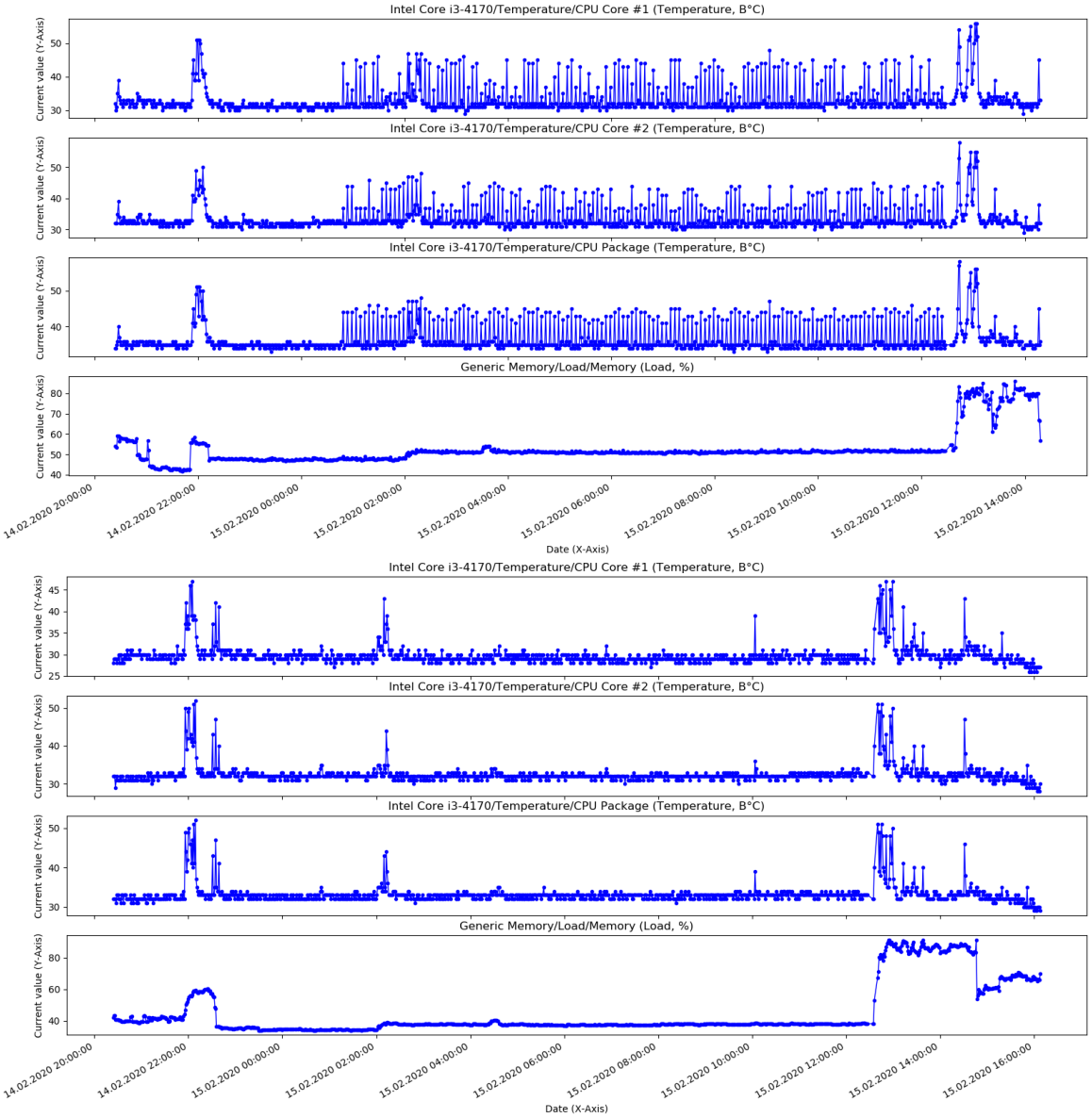

Рис. 2. *Косвенный мониторинг несанкционированной активности двух компьютеров из ста [11]*

памяти не наблюдается. В отдельные временные интервалы процессор занимается чем-то, что мы не можем определить.

В России требования обеспечения безопасности, в том числе и информационной, для систем с критической миссией регламентируются рядом федеральных законов, таких как «О безопасности объектов топливно-энергетического комплекса» (от 21.07.2011 № 256-ФЗ) и «О безопасности критической информационной инфраструктуры Российской Федерации» (от 26.07.2017 № 187-ФЗ). Однако 187-ФЗ допускает возможность инцидентов в значимых объектах критической информационной инфраструктуры. Для парирования возникающих при этом угроз необходимо создание технологий, обеспечивающих штатное функционирование цифровых систем управления в условиях деструктивных внешних и внутренних воздействий.

Проект комплексной научно-технической программы «ФЛАГМАН»

ГК «РОСТЕХ», совместно с ФГУ ФНЦ НИИСИ РАН и ведущими институтами РАН и вузов страны, сформирован проект программы «ФЛАГМАН», который нацелен на решение этой, стратегически важной для обеспечения безопасности страны, проблемы.

Основная цель программы — парирование угрозы перехвата управления и нештатного функционирования систем с критической миссией (СКМ):

- промышленного оборудования:

– добычи, транспортировки и переработки нефти и газа;
– атомных энергетических установок;
– тепловых, газовых и гидравлических турбин;
– электрогенераторов и электроподстанций;
– авиационного и ж/д транспорта;
● сложных технических объектов:
– предприятий нефте- и газодобычи, транспортировки и переработки;
– тепловых, атомных и гидроэлектростанций;
– энергосистем;
– аэропортов и ж/д узлов;
– банков.

Для достижения этой цели необходимо разработать технологии создания:

● цифровых двойников объектов управления (промышленное оборудование, сложные технические объекты); цифровых двойников цифровых систем управления этими объектами, всех их аппаратных и программных компонент и на этой основе — профилей и угроз их штатному функционированию; цифровых двойников возможных киберпротивников на основе, как имеющихся фактических данных об атаках на конкретные объекты, так и данных о возможных прогнозируемых угрозах атак на эти объекты, а также моделей парирования этих угроз;

● интеллектуальных элементной компонентной базы (ЭКБ), средств вычислительной и коммуникационной техники с развитыми средствами самоконтроля и самокоррекции, устойчивых к внешним и внутренним деструктивным воздействиям;

● интеллектуального базового и прикладного программного обеспечения с развитыми средствами самоконтроля и самокоррекции, устойчивых к внешним и внутренним деструктивным воздействиям.

Важнейшим начальным этапом программы является проведение научных исследований с целью создания цифровых двойников: объектов управления, цифровых систем управления этими объектами, включая все основные компоненты (ЭКБ, СВТ, ПО) возможных киберпротивников и на этой основе моделей угроз и их парирования, профилей штатного функционирования.

Синергетический эффект достижения основной цели — крупносерийное производство в России элементной базы и вычислительной техники на ее основе, то есть возрождение радиоэлектронной отрасли России.

ЛИТЕРАТУРА

1. *MalwareTech Botnet Tracker: WCRYPT.* Архивная копия от 13 мая 2017 года. Режим доступа: http://web.archive.org/web/20170513071100/https://intel.malwaretech.com/botnet/wcrypt.
2. *MalwareTech Botnet Tracker: WCRYPT.* Архивная копия от 27 мая 2017 года. Режим доступа: http://web.archive.org/web/20170527061313/https://intel.malwaretech.com/botnet/wcrypt.
3. Эксперты оценили ущерб от вируса WannaCry в $1 млрд. *RuNews24.* Режим доступа: https://runews24.ru/internet/25/05/2017/3deb290a821bd12cc946653ea418e439.
4. *Энциклопедия Интернет-угроз.* Режим доступа: https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/.
5. Барроуз М. *Будущее: рассекречено. Каким будет мир в 2030 году.* М.: Манн, Иванов и Фербер; 2015. 352 с.
6. Червь Stuxnet эксплуатирует четыре 0-day уязвимости. *Anti-Malware.* Режим доступа: https://www.anti-malware.ru/news/2015-12-21/2973.
7. «Газпрому» принудительно отключили импортную технику через спутник. *РБК*. Режим доступа: https://www.rbc.ru/business/15/10/2019/5da5f1e19a7947cfb127bdfd.
8. Атака на систему энергоснабжения Венесуэлы велась из двух городов США. *Российская газета*. 16.03.2019. Режим доступа: https://rg.ru/2019/03/16/ataka-na-sistemu-energosnabzheniia-venesuely-velas-iz-dvuh-gorodov-ssha.html.
9. Петросюк Г. Г., Калачев И. С. О кибербразведке и кибербезопасности КВО. *Кибербезопасность АСУ ТП критически важных объектов*: Онлайн-конференция. Режим доступа: http://www.itsec.ru/adapt/conference17.09.

10. Актуальные киберугрозы: II квартал 2020 года. *POSITIVE TECHNOLOGIES*. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/.
11. Гавриленко Т. В., Никифоров А. В. Методы косвенного мониторинга несанкционированной активности в вычислительных системах. *Вопросы технических и физико-математических наук в свете современных исследований*. 2020;3–4(20):38–45.
12. The Intel 64 and IA-32 Architectures Software Developer's Manual. Vol. 2: Instruction Set Reference, A-Z, Order Number 325383, 2016. 2198 p. Режим доступа: https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf.