Сергей Солдатов

Защита рабочих мест операторов АСУ ТП

С 1 января 2018 года вступает в силу Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». Данный закон устанавливает уголовную ответственность за неправомерный доступ к критической информационной структуре РФ, системам управления технологическими процессами в атомной и химической промышленности, энергетике и оборонно-промышленном комплексе. Несмотря на пользу данного закона как средства предупреждения неправомерного доступа к критическим системам, вопрос о том, как предотвратить взлом, получение и подмену закрытой информации, остаётся во многих аспектах нерешённым (рис. 1). Отдельной проблемой является организация физической безопасности рабочих мест для предотвращения несанкционированных подключений к ним.

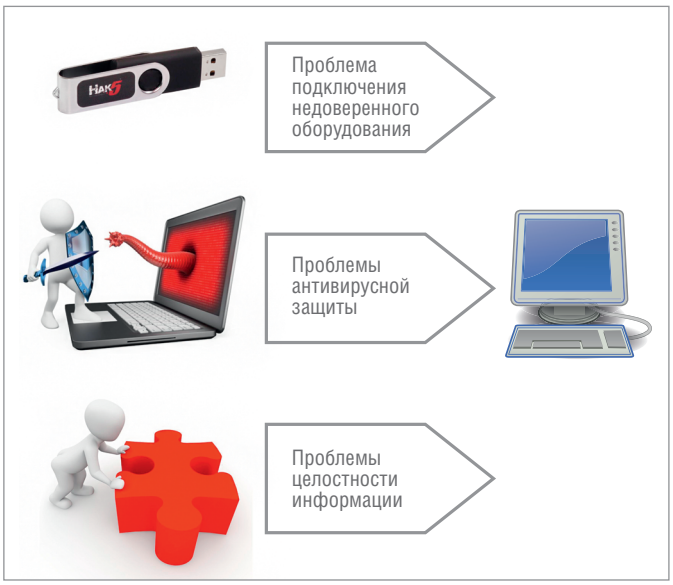

Рис. 1. Проблемы безопасности АРМ оператора АСУ ТП

Проблемы безопасности рабочих мест

Проблема подключения недоверенного оборудования

Технических и программных средств защиты информации огромное количество, зачастую они дублируют друг друга, ещё чаще мешают друг другу. При этом самые простые и элементарные средства физической безопасности защищаемых АСУ ТП игнорируются или им не уделяется должное внимание. В диспетчерских вполне можно увидеть картину, когда к АРМ диспетчера подключён по USB-интерфейсу смартфон сотрудника для его зарядки. Такое подключение сводит на нет все работы по повышению сетевой безопасности. Ни один сетевой экран и антивирус не остановит сотрудника, желающего срочно перекинуть фотографии с телефона на компьютер. В данном случае могут помочь как полная физическая блокировка всех интерфейсов ПК, не используемых для работы, так и административные регламенты, по которым сотрудникам категорически запрещается подключать сторонние технические средства к своим рабочим местам.

Но если с административными регламентами всё прозрачно: разработали, сотрудники подписали, руководство проверяет, то физическая блокировка может быть затруднительна. Конструктив может не позволить демонтировать неиспользуемые порты, демонтаж кабелей связи с портами внутри корпуса требует времени, а иногда и квалификации. К тому же любые изменения в конструкции ПК должны быть согласованы с производителем и системным интегратором, в противном случае есть риск получить отказ в гарантийном обслуживании.

Но иногда задача обеспечения безопасности более сложная, поскольку специфика работы персонала может требовать свободного доступа к интерфейсным портам. Например, сервисному инженеру нужна возможность записывать на карты памяти ПЛК новые версии программ либо считывать с USB-накопителей, снятых с ПЛК или операторских панелей, отчёты и протоколы работы. Как в этом случае обеспечить безопасность?

А что если пользователь просто поменяет одну клавиатуру на другую или поменяет мышь, подключит другой принтер? Будет ли это нарушением безопасности? К сожалению, многие администраторы АСУ ТП, скорее всего, не обратят внимание на данные действия. Да и в регламентах вряд ли будет описана ситуация замены оборудования. Тем не менее, это тоже потенциальная угроза безопасности, так как вновь подключаемое оборудование может быть недоверенным и содержать технические и программные закладки. В более простых случаях оно может оказаться просто неисправным и вызвать из-за неправильной работы паралич системы управления техническим объектом.

Проблемы антивирусной защиты

Антивирусное ПО уже давно стало неотъемлемой частью корпоративного ПО. На рабочих местах бухгалтеров, юристов, менеджеров практически всегда стоит антивирусное ПО. В АСУ ТП антивирусное ПО долгое время не приживалось, но поскольку в последние годы выросла степень интеграции SCADA со смежными системами, появились сложные и

функциональные системы отчётов, а в самих SCADA активно стали использоваться базы данных и скрипты на языках программирования общего назначения, то увеличивается опасность заражения данных систем компьютерными вирусами и антивирусное ПО – это необходимость. Успешно проведённые атаки на ряд индустриальных систем также сподвигли заказчиков и интеграторов обратить больше внимания на антивирусную защиту.

Но, как ни странно, антивирусное ПО тоже надо защищать. Недавний пример взлома специализированного ПО от компании «Лаборатория Касперского», предназначенного для защиты от взлома и вирусной атаки на банкоматы, наглядно показал, как важно обеспечить безопасность антивирусного и другого ПО для защиты ПК [1]. Вредоносные программы типа rootkit, работающие на уровне ядра ОС, могут успешно скрывать себя от антивируса, а в некоторых случаях отключать его или даже использовать после модификации для загрузки других вирусов. Чтобы обнаружить подобные вирусы, необходимо выполнять проверку ПК, загрузившись с изолированного от проверяемой системы носителя до загрузки рабочей ОС. Но не будет же пользователь каждый раз загружаться со специальной флэшки и проверять систему. Есть ли более технологичное решение?

Незнакомые данные

Вы работали на ПК, сохранили данные, а на следующий день увидели, что данные отличаются, но дата и время сохранения те же. Как такое может быть? На самом деле такое вполне возможно, современные файловые системы – это по сути специализированные базы данных, которые может отредактировать любой имеющий права доступа к ним. Таким образом, нарушитель может скрыть изменение какой-либо информации. Но можно ли как-то ещё проконтролировать, менялись ли данные, кроме записей в файловой системе?

Другая ситуация: коллега просит загрузить обновление на ПЛК, он скачал его с сайта производителя. Есть сомнения, точно ли этот файл с сайта производителя. Но как проверить? Есть ли способ убедиться в достоверности источника файла?

Повышение безопасности рабочих мест

Контроль целостности оборудования

Ранее были обозначены несколько проблем контроля подключения недоверенных устройств к рабочим местам операторов/диспетчеров АСУ ТП. Основным способом решения данных проблем является составление списков разрешённого к подключению оборудования с последующей проверкой подключаемого оборудования на соответствие данным спискам. Подобные системы называются системами или средствами контроля целостности оборудования (СКЦО). Для идентификации оборудования служат данные, считываемые из встроенного программного обеспечения оборудования: производитель, модель устройства, серийный номер. В зависимости от реализации СКЦО при подключении недоверенного оборудования возможна как полная блокировка работы ПК, так и игнорирование устройства при работе ПК, как будто ничего не подключали. Возможен также контроль отключения доверенных устройств, например, при отключении штатной клавиатуры рабочее место будет автоматически заблокировано.

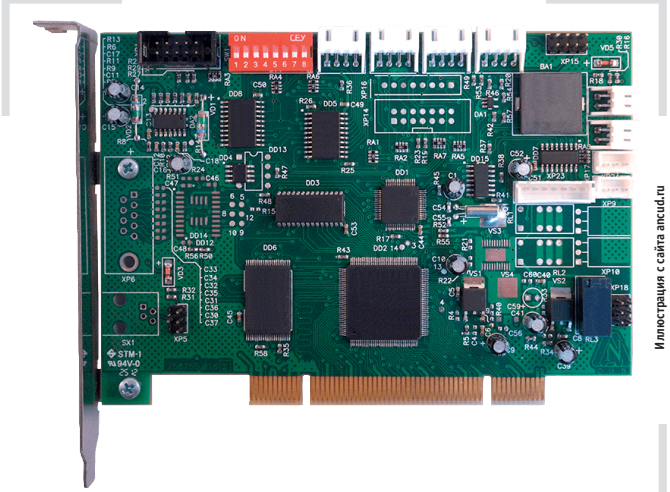

Иллюстрация с сайта ancud.ru

Рис. 2. Аппаратно-программный модуль доверенной загрузки «КРИПТОН-ЗАМОК/У»

Контроль целостности оборудования может осуществляться на разных этапах работы ПК: непосредственно при загрузке ПК и во время работы ПК. Первый вариант наиболее распространён и поддерживается во многих средствах аппаратной защиты. Если к системе подключили недоверенное устройство, ПК будет бесконечно перезагружаться в ожидании устранения нарушения контроля целостности или будет автоматически выключен. В обоих случаях будет выводиться информационное сообщение о нарушении целостности.

Наиболее часто контроль целостности оборудования реализуется за счёт применения специализированных модулей безопасности, которые представляют собой либо самостоятельные устройства (рис. 2), устанавливаемые в слоты PCI/miniPCI [2, 3], либо интегрируемые непосредственно в материнскую плату. Подобные системы способны не только контролировать целостность оборудования, но и выполнять аутентификацию и авторизацию пользователей, постоянный мониторинг состояния оборудования ПК в процессе его работы, криптографические операции (шифрование/дешифрование, вычисление хеша, операции с электронными цифровыми подписями).

Но стоит отметить, что аппаратные решения имеют довольно высокую стоимость, что ограничивает их сферу применения прежде всего государственными органами, преимущественно силовыми ведомствами, и крупным бизнесом. Для большинства компаний основными средствами контроля целостности аппаратного обеспечения являются программные средства.

Программный контроль может быть трёх видов: с использованием средств ОС, с использованием специализированных программ, с использованием гипервизора. Так, в ОС Windows можно выполнить настройку блокировки USB-устройств, причём как полную [4], так и частичную, например, для всех USB-накопителей, кроме разрешённых [5], или вовсе запретить все USB-накопители [6]. Для Linux также существует возможность, используя встроенные средства, заблокировать USB-накопители [7].

Применение специализированных программ даёт администраторам больше возможностей по блокировке недоверенных устройств и управлению оборудованием рабочих мест [8]. В таких средствах зачастую есть удалённый контроль и настройка доступа к устройствам для рабочих мест, что позволяет оперативно перенастраивать рабочие места.

Наиболее удобным видится контроль с использованием гипервизора. Гипервизор – это программа, обеспечивающая одновременную работу нескольких операционных систем на одном физическом компьютере. Помимо разделения аппарат-

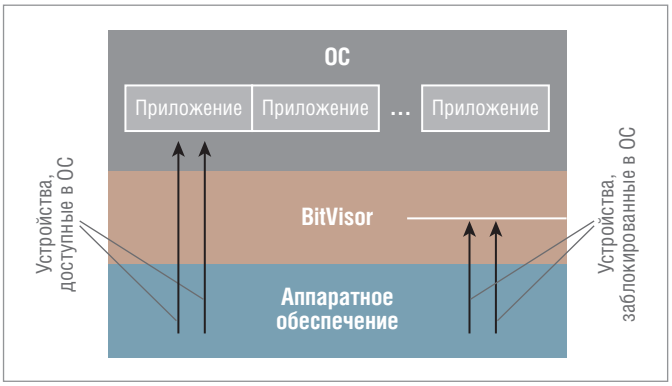

Рис. 3. Упрощённая структурная схема BitVisor

ных ресурсов гипервизор обеспечивает изоляцию нескольких ОС друг от друга, а также их защиту и безопасность. Гипервизор может эмулировать физические устройства, а также скрывать их от ОС. Последнее и представляет наибольший интерес при обеспечении безопасности на отдельном рабочем месте. Полноценный гипервизор здесь уже не нужен, его функции минимальны, хотя и не менее сложны, он должен выполнять мониторинг обмена между ОС и физическим оборудованием и при соответствующих настройках ограничивать доступ ОС к аппаратному обеспечению [9], как показано на рис. 3, например, предоставлять доступ только на чтение или выполнять шифрование/дешифрование на лету [10].

Основную сложность при внедрении гипервизора представляет необходимость разработки драйверов для каждого из устройств, которое планируется контролировать. Поэтому подобные программные средства в основном поставляются комплектно с аппаратным обеспечением ПК. В противном случае придётся заказывать разработку драйверов или выполнять её самостоятельно. В то же время ограничений на выбор используемых ОС у заказчика практически нет. Да и сам процесс установки, настройки и работы с ОС на ПК с таким гипервизором ничем не отличается от работы с обычным ПК.

Контроль целостности данных

Информацию можно подделать – данный постулат не требует опровержения. Поэтому средства контроля целостности – неотъемлемая часть современной ИТ-инфраструктуры. Самый простой способ – создать копию, но и самый слабый в смысле безопасности – копию можно подделать так же, как оригинал.

Более надёжный и компактный по размеру способ – расчёт контрольной суммы. Данное понятие хорошо известно в АСУ ТП, поскольку ни один промышленный протокол передачи информации не обходится без расчёта контрольной суммы пакета данных. Наиболее известен алгоритм расчёта циклического избыточного кода (CRC – Cyclic Redundancy Check). Но в силу простоты алгоритма для разных данных возможны идентичные CRC, что позволяет подделывать их, поэтому контрольные суммы – хороший способ повышения помехоустойчивости, но не более того.

Следующим по надёжности идёт вычисление хеша данных (hash). Hash-алгоритмы преобразуют входные данные произвольной длины в битовую строку фиксированного размера [11]. Функция, реализующая данный алгоритм, называется hash-функцией. Любое изменение входных данных меняет вычисленное значение. Одно из преимуществ хеша данных – это его компактность. Другое преимущество – стойкость. Хорошая hash-функция не имеет коллизий (уникальное вычисленное значение для разных наборов данных), или их поиск занимает значительное время. Недостаток hash-функций – более высокие требования к вычислительной мощности. Тем не менее, данный способ контроля целостности информации получил наибольшее распространение.

Развитием hash-алгоритмов можно назвать электронную цифровую подпись. Здесь также вычисляется хеш данных, но он ещё и шифруется с использованием асимметричного шифрования (шифрование одним ключом – закрытым, расшифровка другим – открытым). Автор генерирует ключи шифрования и расшифровки, закрытый хранит у себя, открытый передаёт адресату. Это позволяет не только контролировать целостность данных, но и определять авторство. Открытый и закрытый ключи связаны между собой, и если автор не тот, за кого выдаёт себя, то предоставленный настоящим автором ключ не подойдёт для расшифровки хеша данных (рис. 4). Поскольку при передаче открытого ключа нет гарантии, что его никто не подделал, была разработана инфраструктура открытых ключей и сертификатов удостоверяющих центров. Тогда с сообщением передаётся не только подпись, но и сертификат, удостоверяющий её [12].

Антивирусная защита до загрузки ОС

Антивирусная защита прочно вошла в набор программ рядового пользователя. Этому способствовали как повышение грамотности пользователей, так и ряд компьютерных эпидемий, прокатившихся по миру [13]. Но антивирусная защита, к сожалению, не всегда способна обезопасить сами антивирусы. Rootkit (руткит) – вредоносные программы, скрывающие себя от глаз пользователя и антивирусов. Наибольшую угрозу представляют те, что работают на уровне ядра ОС и имеют максимальный уровень прав доступа. После инсталляции такой программы возможности атакующего практически безграничны. Создание rootkit уровня ядра обычно крайне сложный процесс, но обнаружить и удалить его на порядок сложнее. Поскольку ядро ОС запускается намного раньше антивируса, то rootkit уровня ядра легко может блокировать работу антивируса, не допустив обнаружения. Пользователь

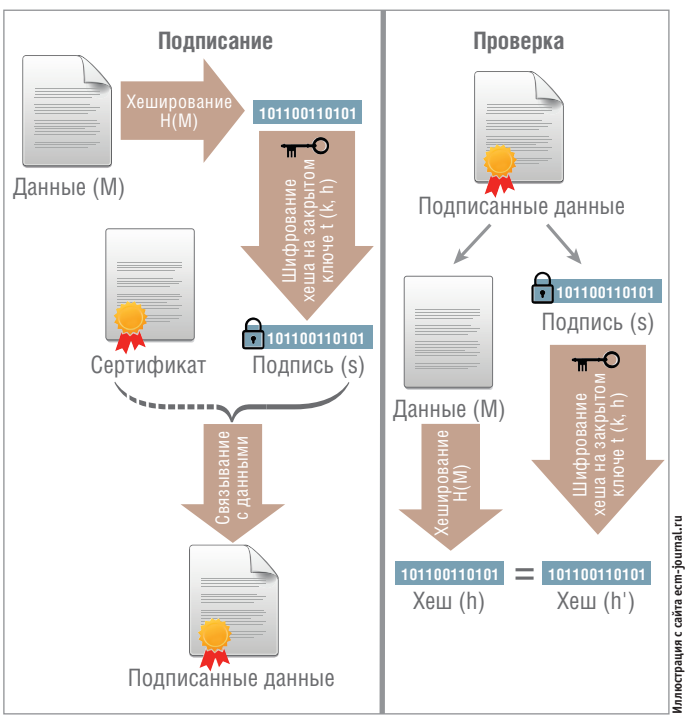

Рис. 4. Подписание данных с помощью электронной цифровой подписи и их проверка

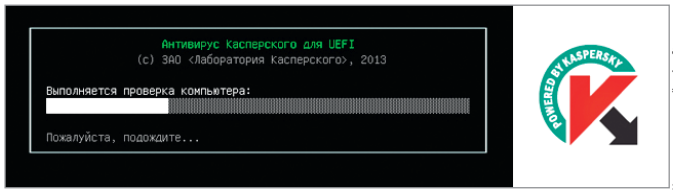

Иллюстрация с сайта kraftway.ru

Рис. 5. Окно проверки компьютера антивирусом Касперского для UEFI

узнаёт о заражении только по косвенным признакам: подозрительной загрузке процессора, загрузке памяти, сетевой активности. Борьба с такими программными средствами – сложный процесс, к сожалению, часто оканчивающийся полной переустановкой ОС. Тем не менее, защититься от данных вредоносных программ можно.

Как было сказано, «хороший» rootkit имеет привилегии и запускается до антивируса, чтобы избежать своего обнаружения. Но что, если запустить антивирус до загрузки ОС, когда rootkit ещё не стартовал? Практически все антивирусные разработчики выпускают загрузочные образы, которые можно установить на USB-носитель и с их помощью загрузить ПК и проверить его на вирусы. Сигнатурный анализ (определение вредоносных программ по определённым участкам машинного кода) позволит выявить rootkit и удалить его. Конечно, после этого, скорее всего, потребуется провести дополнительную проверку антивирусом, уже загрузившись с встроенного в ПК носителя, но «зловред», скорее всего, будет уже ослаблен и появится возможность удалить вирус.

Всё хорошо, но только это неудобно для пользователя. Вставлять сторонний носитель, задавать загрузочный носитель, выполнять проверку, перезагружать ПК – всё это множество операций, в которых пользователь или ошибётся, или пропустит один из шагов.

Компания «Лаборатория Касперского» предложила новое решение – антивирус Касперского для UEFI (KUEFI) [14]. Новый антивирус Касперского для UEFI (Unified Extensible Firmware Interface) обеспечивает безопасную загрузку компьютера (рис. 5), проверяя системные файлы на наличие в них вредоносного кода ещё до начала работы ОС и основного антивируса. UEFI – это новый этап развития хорошо известной BIOS (Basic Input/Output System – базовая система ввода-вывода), которая есть во всех материнских платах. UEFI, так же как BIOS, выполняется до загрузки ОС, проводит инициализацию устройств ПК, обеспечивает настройку работы ПК. Но есть и существенные отличия от BIOS: возможность работы по сети, графический интерфейс, работа с дисками большого размера (более 2,2 Тбайт) и др. По сути, это мини-ОС, для которой можно написать свои приложения и разместить их во флэш-памяти на материнской плате.

Благодаря работе на уровне EFI BIOS KUEFI обеспечивает эффективную защиту от руткитов, буткитов (программы, подменяющие загрузочные данные ОС) и угроз, разработанных специально для обхода технологий защиты классических антивирусов.

Определённой альтернативной KUEFI может служить ранний запуск антивредоносной программы, предложенный в ОС Windows 10 [15]. Традиционные антивредоносные приложения не запускаются до тех пор, пока не будут загружены драйверы загрузки, что позволяет сработать руткиту, замаскированному под драйвер. Ранний запуск антивредоносной программы (ELAM – Early Launch Anti-malware) может загрузить драйвер антивредоносного ПО Microsoft или сторонних разработчиков перед загрузкой всех драйверов и приложений загрузки, отличных от Microsoft. У ELAM простая задача: изучить каждый драйвер загрузки и определить, входит ли он в список надёжных драйверов. Если он не считается доверенным, Windows его не загружает.

Заключение

В данной статье были затронуты только три направления защиты АРМ операторов АСУ ТП, и, безусловно, нельзя ограничиваться только ими. Есть потребности в сетевой защите, защите от съёма излучений с портов ПК, в организационных и административных мероприятиях и т.п. Но, тем не менее, описанные решения по повышению информационной безопасности показывают, что средства защиты не стоят на месте и сложности взлома и кражи данных постоянно растут, а значит, противостояние щита и меча продолжится. ●

Литература

1. Hack ATM with an anti-hacking feature and walk away with $1M in 2 minutes [Электронный ресурс] // Режим доступа : https://embedi.com/wp-content/uploads/dlm_uploads/2017/11/Hack-ATM-with-an-anti-hacking-feature-and-walk-away-with-1M-in-2-minutes-1.pdf.
2. Модельный ряд «Соболь» [Электронный ресурс] // Режим доступа : https://www.securitycode.ru/products/pak_sobol/models/.
3. Trusted Security Module (TSM) [Электронный ресурс] // Режим доступа : https://www.aladdin-rd.ru/catalog/tsm.
4. Как отключить или включить USB-порты в Windows [Электронный ресурс] // Режим доступа : http://compconfig.ru/winset/kak-otklyuchit-ili-vklyuchit-usb-portyi-v-windows.html.
5. Безмалый В. Управление внешними запоминающими устройствами в Windows 7 [Электронный ресурс] // Режим доступа : https://technet.microsoft.com/ru-ru/library/ee922727.aspx.
6. Предотвращение использования USB-устройств хранения данных [Электронный ресурс] // Режим доступа : https://support.microsoft.com/ru-ru/help/823732/how-can-i-prevent-users-from-connecting-to-a-usb-storage-device.
7. Мониторинг подключения USB-накопителей и логирование операций с файлами [Электронный ресурс] // Режим доступа : https://habrahabr.ru/post/223363/.
8. Block or allow devices in Endpoint Protection [Электронный ресурс] // Режим доступа : https://support.symantec.com/en_US/article.TECH175220.html.
9. BitVisor Manual [Электронный ресурс] // Режим доступа : https://sourceforge.net/projects/bitvisor/files/bitvisor/documents/manual/bitvisor-1.1-manual-japanese.pdf/download.
10. Trevisor [Электронный ресурс] // Режим доступа : https://github.com/lakeman/trevisor.
11. Чудеса хеширования [Электронный ресурс] // Режим доступа : https://www.kaspersky.ru/blog/the-wonders-of-hashing/3633/.
12. Рудин С. Кратко об электронной подписи, ключах и сертификатах [Электронный ресурс] // Режим доступа : https://ecm-journal.ru/docs/Kratko-ob-ehlektronnojj-podpisi-kljuchakh-i-sertifikatakh.aspx.
13. Самые масштабные и значимые атаки компьютерных вирусов в мире. Досье [Электронный ресурс] // Режим доступа : http://tass.ru/info/4248876.
14. Kaspersky Anti-Virus for UEFI [Электронный ресурс] // Режим доступа : https://www.kaspersky.ru/antivirus-for-uefi.
15. Защита процесса загрузки Windows 10 [Электронный ресурс] // Режим доступа : https://docs.microsoft.com/ru-ru/windows/threat-protection/secure-the-windows-10-boot-process.

E-mail: ssa-company@rambler.ru