DOI 10.23859/1994-0637-2017-4-79-1
УДК 004.056.52

Артемов Николай Игоревич
Инженер, Череповецкое высшее военное инженерное училище радиоэлектроники (Череповец, Россия)
E-mail: anilead@mail.ru

Сотников Александр Иванович
Преподаватель, Череповецкое высшее военное инженерное училище радиоэлектроники (Череповец, Россия)
E-mail: vokintos@rambler.ru

Асеев Алексей Юрьевич
Кандидат технических наук, доцент Череповецкий государственный университет, (Череповец, Россия)
E-mail: passionarij@rambler.ru

Artemov Nikolay Igorevich
Engineer, Cherepovets Higher Military College of Radioelectronics (Cherepovets, Russia)
E-mail: anilead@mail.ru

Sotnikov Aleksandr Ivanovich
Teacher of the Department of Information Security, Cherepovets Higher Military College of Radioelectronics (Cherepovets, Russia)
E-mail: vokintos@rambler.ru

Aseev Aleksey Urievich
PhD (Technology), associate professor, Cherepovets State University, (Cherepovets, Russia)
E-mail: passionarij@rambler.ru

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОГО КЛАСТЕРА С ПОМОЩЬЮ МЕТОДА «КОНТРОЛЬНОГО ПАКЕТА»

SECURITY OF THE PROTECTED CLUSTER WITH THE METHOD OF "CONTROL PACKAGE"

Аннотация. В данной статье рассмотрена проблема и предложено решение организации защиты критически важных объектов от внешних угроз, реализуемых с помощью USB-накопителей. Решение представляет собой систему защиты, проверяющую принадлежность накопителей к защищаемому кластеру, права пользователя на использование USB-накопителей, а также содержимое накопителей на предмет несанкционированного его изменения. Результатом реализации данной системы защиты является специальное программное обеспечение «USB Protect System».

Ключевые слова: защита информации, безопасность, USB, целостность, несанкционированное изменение, права доступа

Abtract. This article discusses the problem and the ways to protect crucial objects against external threats implemented with of USB-drives. The solution is a security system that verifies the belonging of the drives to the protected cluster, user's right for using USB-drives as well as the contents of the drives for unauthorized modification. The result of this protection system implementation is the special software “USB Protect System”.

Keywords: data protection, security, USB, integrity, unauthorized modification, access rights, software

Введение

В настоящее время особую важность представляют вопросы обеспечения безопасности цифровой инфраструктуры критически важных объектов (КВО). Учитывая высокий процент автоматизации жизнедеятельности государственных структур, нарушение работоспособности систем управления может привести к катастрофическим последствиям. В качестве подтверждения можно привести следующие примеры: использование вируса “Stuxnet”, направленного против ядерной программы Ирана; получение доступа к конфиденциальной переписке директора ЦРУ с дальнейшим размещением скомпрометированной информации на сайте “Wikileaks” [5].

Особенностью эксплуатации большинства КВО является специфическое взаимодействие системы с внешними миром, которое проявляется в отсутствии или жестком ограничении на подключение объектов к глобальной сети Интернет и другим информационно-телекоммуникационным системам. Как следствие, использование мобильных накопителей информации (МНИ) становится неотъемлемой частью работы внутри КВО. С одной стороны, это повышает безопасность защищаемого кластера в целом, с другой, – доверенное использование накопителей информации внутри защищаемого кластера в некоторых случаях может привести к нарушению функционирования элементов КВО. Одной из наиболее опасных угроз в данном случае является возможность внедрения в основные и вспомогательные технические средства КВО вредоносного или потенциально опасного программного обеспечения при использовании незарегистрированных накопителей или одновременной эксплуатации зарегистрированных МНИ внутри защищаемого кластера и за его пределами.

Основная часть

По материалам открытых источников был проведен анализ реализации угроз персональным компьютерам (ПК) организации посредством USB-накопителей. Одним из фактов, подтверждающих высокую вероятность злонамеренного или халатного использования МНИ обычными пользователями, является исследование, проведенное компанией “SanDisk” в США, в котором в качестве объектов выступали рядовые сотрудники организаций и IT-специалисты. При проведении эксперимента было установлено, что 77 % респондентов используют личные USB-накопители для хранения и переноса служебной информации, причем 12 % сотрудников компании находили USB-накопители в общественных местах и 55 % из них пробовали посмотреть хранящуюся на нем информацию. В то же время в Великобритании проводился «обратный» эксперимент. Суть его заключалась в том, что в общественных местах, местах для курения, на автозаправках, рядом с предприятиями оставляли USB-накопители содержащие вредоносное ПО. Результат показал, что 95 % людей воспользовались данными USB-накопителями на корпоративных машинах [1].

Учитывая проведенный анализ, можно выделить два основных вида угроз, реализуемых с помощью мобильных накопителей информации:

1. Воздействие на инфраструктуру организации при использовании содержимого, созданного или измененного за пределами кластера ПК организации. Данная угроза может быть реализована следующими способами:

а) подключением к ПК организации неучтенных USB-накопителей;

б) использованием содержимого (ПО, документы, HTML-страницы), полученного за пределами организации и принесенного на учтенном USB-накопителе.

2. Утечка служебной информации за пределы организации. Данный вид угрозы может быть реализован посредством:

а) копирования служебной информации на несанкционированные USB-накопители;

б) копирования информации на санкционированный накопитель с последующим использованием его вне защищенного кластера.

Противодействовать данным угрозам возможно при решении следующих задач:

– запретить подключение к ПК неучтенных USB-накопителей;

– запретить возможность использования на ПК организации зарегистрированных USB-накопителей, если произошло изменение целостности содержания, произведенного вне защищаемого кластера.

В настоящее время данные задачи решаются с помощью организационных и программных механизмов защиты, примеры которых представлены в таблице [3]:

Таблица

Механизмы защиты от угроз, реализуемых с помощью накопителей информации

Опасность	Механизмы защиты
Возможность использования МНИ вне организации	Установка различных систем защиты информации, допускающих использование только строго определенных (зарегистрированных) МНИ. Настройка правил разграничения доступа при работе МНИ
Возможность НСД к ПК организации путем использования программ, размещенных на МНИ вне защищенного кластера	Использование антивирусных программ, настройка системы разграничения доступа (запрета запуска программ, отсутствующих в разрешенном списке; проверки целостности программ перед запуском; замены поврежденных программ резервными копиями по результатам проверки)
Файлы на накопителе информации могут быть несанкционированно удалены или изменены	Снабжение накопителей информации средствами аутентификации пользователя или применение криптографических методов защиты данных, записываемых на эти носители

В качестве недостатков данных механизмов защиты можно выделить:

– при реализации СЗИ, допускающих строго определенные МНИ, требуется использование ЛВС с базой данных зарегистрированных МНИ на ПК администратора или отдельных баз данных на каждом ПК организации, что приводит к дополнительным временным и финансовым затратам в случае необходимости внести или изменить данные о разрешенных мобильных накопителях информации;

– криптографические методы защиты данных не обеспечивают защиту от несанкционированного злонамеренного изменения или удаления данных владельцем МНИ;

– невозможно ограничить использование информации, полученной сотрудником организации за ее пределами и размещенной на учтенный МНИ;

– снабжение МНИ средствами аутентификации пользователя не решает проблемы искажений или удаления информации при обработке легальным пользователем (злонамеренной или в результате работы на враждебном ПК);

– антивирусы не дают гарантированной защиты, а только снижают риск [5].

Основываясь на данных фактах, можно сделать вывод, что на сегодняшний день в открытом доступе не представлено достаточно эффективного и удобного решения,

способного обеспечить комплексную безопасность использования мобильных накопителей информации в организации.

Для решения задачи запрета использования незарегистрированных носителей, а также носителей, изменение содержания которых было произведено вне защищаемого кластера, предлагается система защиты на основе метода «контрольного пакета».

Система защиты на основе метода «контрольного пакета» – это совокупность политик, правил и программных механизмов работы с мобильными накопителями информации, направленных на:

– проверку мобильных носителей информации;

– запрет на эксплуатацию МНИ в пределах защищаемого кластера в случае определения фактов использования незарегистрированных устройств или несанкционированного изменения содержания данного носителя.

Обобщенная схема работы предлагаемой системы защиты представлена на рис. 1.

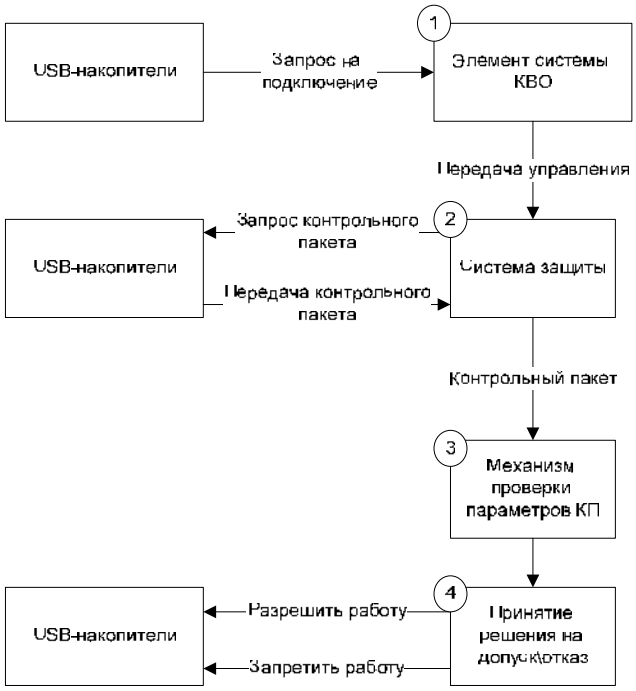

Рис. 1. Обобщенная схема работы системы защиты

Принцип функционирования предложенной системы защиты заключается в следующем. При инициализации накопителя информации на элементе системы происходит передача управления над USB-накопителем системе защиты. Система защиты представляет собой специальное программное обеспечение, которое блокирует все информационные потоки между USB-накопителем и элементом КВО до завершения процедуры проверки (1). Система защиты запрашивает доступ к контрольному пакету, который находится внутри содержимого USB-накопителя (2). При получении доступа к нему происходит сравнение параметров контрольного пакета с параметрами, рассчитанными механизм защиты (3).

На основании результата проверки система защиты принимает решение (4) на разрешение или запрет работы с USB-накопителями и передает управление обратно.

Контрольный пакет представляет специально сформированный при регистрации USB-накопителя блок данных, который основан на двух параметрах: статическом и динамическом (рис. 2).

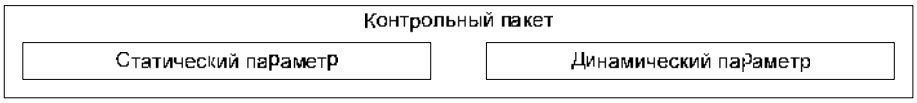

Рис. 2. Параметры контрольного пакета

Статический параметр представляет собой совокупность идентификатора защищаемого кластера и аутентификатора пользователя, которые однозначно определяют принадлежность накопителя информации к защищаемому кластеру и права пользователя на использование данного накопителя на КВО.

Основной задачей статического параметра является обеспечение механизма защиты всеми информационными ресурсами, необходимыми для принятия решения о принадлежности мобильного накопителя информации к защищаемому кластеру и правомерности его использования данным пользователем.

Динамический параметр предназначен для контроля целостности содержания данных информационного потока, и его изменение в контрольном пакете должно производиться при каждом использовании накопителя информации на элементе защищаемой системы.

Формирование данного параметра осуществляется путем расчета значений, характеризующих целостность:

- основного содержания USB-накопителя;
- полного содержания USB-накопителя.

Таким образом, сформированный контрольный пакет представляет собой блок данных, включающий совокупность рассчитанных параметров и представленных в виде символьной последовательности. Для интеграции в информационный поток в мобильном накопителе информации необходимо выделить свободное пространство, которое должно быть скрыто от пользователей, а доступ к нему должен быть разрешен только механизму защиты. Наиболее рационально будет осуществить интеграцию контрольного пакета в мета-поток информационного потока МНИ.

Мета-поток – это скрытый управляющий информационный поток основного потока информации, который используется для синхронизации с объектом при инициализации МНИ, а также для управления информационным потоком и его описания (например, NTFS-поток, который отражает структуру файловой системы с содержащейся в ней информацией). Полный механизм формирования контрольного пакета представлен на рис. 3.

Первое формирование контрольного пакета и встраивание его в мета-поток должно производиться на специально выделенном объекте защищаемого кластера, который является буфером между внешней средой и элементами защищаемого кластера. Данный объект должен находиться внутри кластера, но не принадлежать к группе элементов критически важных объектов.

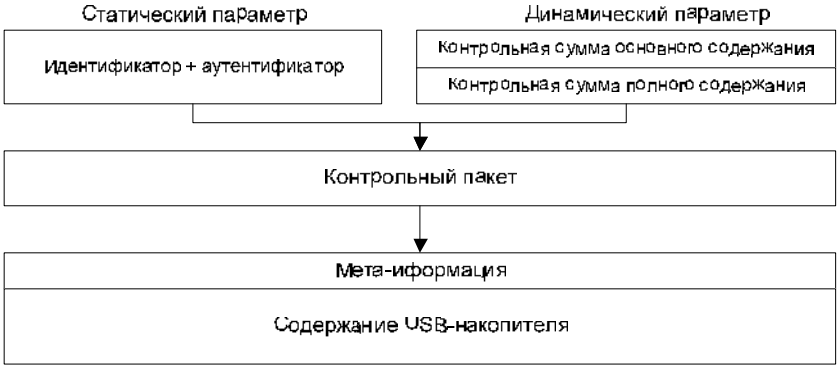

Рис. 3. Формирование и интеграция контрольного пакета

После встраивания контрольного пакета в мета-поток система защиты запрещает доступ к информации, содержащейся в нем для любого пользователя, кроме самой системы защиты. Достигается это путем полного перехвата обращения ОС к МНИ системой защиты при каждой его инициализации на любом элементе защищаемого кластера.

После формирования контрольного пакета и интеграции его в структуру МНИ накопитель информации будет считаться зарегистрированным (учтенным) и предназначенным для работы внутри защищаемого кластера.

Выводы

В данной работе была рассмотрена проблема возможности несанкционированного размещения на элементах защищаемой системы данных, полученных за пределами организации, предложено ее решение, основанное на внедрении в содержание накопителя специально сформированного пакета данных и его проверке при каждом использовании МНИ. Данный механизм защиты был реализован в прототипе СПО “USB Protect System”. Тестирование данного прототипа в реальных условиях показало высокий уровень защиты от рассмотренной угрозы.

Литература

1. Артемов Н.И., Сотников А.И. Исследование механизмов защиты персональных компьютеров от угроз, реализуемых с помощью USB-накопителей. Череповец: ЧВИУРЭ, 2015.

2. Кулаков В.К. Программирование на аппаратном уровне. СПб.: Питер, 2003.

3. Материалы Межрегиональной научной конференции IX ежегодной научной сессии аспирантов и молодых ученых. Вологда: ВоГУ, 2015. Т. 1: Технические науки. Экономические науки. С. 31–35.

4. Руссинович М., Соломон Д., Ионеску А. Внутреннее устройство Microsoft Windows. Основные подсистемы ОС. СПб.: Питер, 2014.

5. Xakep. URL: https://xakep.ru.

References

1. Artemov N.I., Sotnikov A.I. *Issledovanie mekhanizmov zashchity personal'nykh komp'iuterov ot ugroz realizuemykh s pomoshch'iu USB-nakopitelei* [Investigation of mechanisms of protection of personal computers from threats realized with the help of USB-drives]. Cherepovets: ChVVIURE [CVVIUR], 2015.

2. Kulakov V.K. *Programmirovanie na apparatnom urovne* [Programming at the hardware level: a special directory]. St-Petersburg: Piter, 2003.

3. *Materialy Mezhregional'noi nauchnoi konferentsii IX ezhegodnoi nauchnoi sessii aspirantov i molodykh uchenykh* [Proceedings of the Interregional Scientific Conference of the 9th Annual Scientific Session of Postgraduate Students and Young Scientists]. Vologda: VoGU, 2015. T. 1. Tekhnicheskie nauki. Ekonomicheskie nauki. Pp. 31–35.

4. Russinovich M., Solomon D., Ionesku A. *Vnutrennee ustroistvo Microsoft Windows. Osnovnye podsistemy OS* [The internal Microsoft Windows device. The main subsystems of the OS]. St-Petersburg: Piter, 2014.

5. *Xakep* [Online magazine Xakep]. Available at: https://xakep.ru.

Артемов Н.И., Сотников А.И., Асеев А.Ю. Обеспечение безопасности защищаемого кластера с помощью метода «контрольного пакета» // Вестник Череповецкого государственного университета. 2017. №4(79). С. 7–13.

For citation: Artemov N.I., Sotnikov A.I., Aseev A.U. Security of the protected cluster with the method of “control package”. *Bulletin of the Cherepovets State University*, 2017, no. 4 (79), pp. 7–13.