ПРОГРАММНЫЙ КОМПЛЕКС УПРАВЛЕНИЯ ДОСТУПОМ USB-УСТРОЙСТВ К АВТОМАТИЗИРОВАННЫМ РАБОЧИМ МЕСТАМ

Баев А.В.[1], Гаценко О.Ю.[2], Самонов А.В.[3]

В настоящее время для подключения к компьютерам каких-либо внешних устройств, начиная с флеш-накопителей, фото и видео камер и заканчивая офисным оборудованием и сложнейшими медицинскими приборами, все более и более активно используется последовательный интерфейс передачи данных USB. Широкое использование USB-устройств для хранения и передачи данных обусловлено их универсальностью, надежностью, производительностью, простотой и удобством. В тоже время USB-устройства являются одними из наиболее опасных и активно используемых средств и каналов реализации угроз информационной безопасности.

Целью *исследования, результаты которого представлены в данной статье, является повышение защищенности автономных автоматизированных рабочих мест от угроз информационной безопасности, реализуемых с помощью USB-устройств.*

Методы исследования: *для достижения данной цели были исследованы технические характеристики и функциональные возможности USB-устройств, определены потенциальные уязвимости и способы их эксплуатации для реализации угроз информационной безопасности, а также проанализированы достоинства и недостатки существующих подходов и средств защиты.*

Результат *проведенных исследований и работ: создан программный комплекс управления доступом USB-устройств, обеспечивающий защиту автономных автоматизированных рабочих мест, функционирующих под управлением ОС Windows, посредством обнаружения подключаемых устройств, проверки их легитимности по защищенной базе данных о разрешенных USB-устройствах, блокировки нелегитимных подключений, регистрации связанных с этими операциями событий. Данный программный комплекс может также применяться для обнаружения фактов нелегитимного использования USB-устройств, отслеживания и регистрации выполненных с их помощью операций для выявления и анализа инсайдерской деятельности. Дано описание состава, структуры и алгоритмов функционирования данного программного комплекса. Определены основные направления его развития и совершенствования.*

Ключевые слова: *алгоритмы и средства защиты, управление доступом, USB-устройства, уязвимости USB, угрозы информационной безопасности.*

DOI: 10.21681/2311-3456-2020-01-52-61

Введение

Широкое применение USB-устройств для хранения и передачи данных обусловлено тем, что они обладают рядом преимуществ перед другими носителями информации. Основными из них являются: простота использования, мобильность, компактность, высокая скорость, надежность, низкое энергопотребление и широкая аппаратная поддержка на различных платформах. Это, в свою очередь, привело к тому, что USB-устройства стали одними из наиболее опасных и активно используемых средств и каналов реализации угроз информационной безопасности (ИБ).

Данный факт подтверждают результаты целого ряда исследований. Например, в отчете компании Honeywell Industrial Cyber Security[4], которая специализируется в области промышленной кибербезопасности, представлены следующие результаты анализа уязвимостей USB-устройств и связанных с ними угроз ИБ. В результате обследования 50 предприятий из четырех индустриальных областей, расположенных на четырех континентах, было установлено, что на 44% используемых USB-устройств был выявлен и заблокирован, как минимум, один файл, угрожавший безопасности. При этом 26% из этих файлов представляли угрозу, в случае реализации которой операторы могли потерять возможность контролировать состояния объектов и управлять технологическими процессами. Среди обнаруженных угроз были

1 Баев Алексей Владимирович, старший научный сотрудник, Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург, Россия, E-mail: baih@mail.ru

2 Гаценко Олег Юрьевич, доктор технических наук, старший научный сотрудник, АО НИИ ПС, Санкт-Петербург, Россия, E-mail: gatcenko@mail.ru

3 Самонов Александр Валерьянович, кандидат технических наук, доцент, Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург, Россия, E-mail: a.samonov@mail.ru ORCID: 0000-0002-0390-4481

4 https://www.automation.com/pdf_articles/honeywellps/Honeywell-USB-Threat-Report.pdf

такие, как TRITON, Mirai, разные формы червя Stuxnet. В отчете отмечается, что традиционные средства защиты от вредоносных программ не смогли обнаружить 11% выявленных угроз. О значительном росте (более чем в два раза) инцидентов ИБ в РФ, связанных с утечками конфиденциальной информации посредством USB-носителей, сообщается в аналитическом отчете отечественной компании InfoWatch[5].

Для противодействия этим угрозам ИБ используются два подхода. Первый подход предполагает полный запрет и отключение физической возможности использования USB-устройств. Реализация данного решения целесообразна для систем, хранящих и обрабатывающих информацию, содержащую сведения, составляющие государственную тайну или особо конфиденциальные данные. Второй подход основан на использовании программных и аппаратно-программных средств защиты от несанкционированного доступа (СЗИ НСД) и реализации соответствующих организационно-технических мер. СЗИ НСД различаются по составу и способам реализации функциональных возможностей, программно-аппаратным платформам, масштабируемости, сложности установки и эксплуатации, стоимостным и другим характеристикам. Примерами комплексных решений являются такие системы, как «Secret Net», «Страж NT», «Dallas Lock», «DeviceLock DLP». Данные системы обладают необходимым набором функций для противодействия угрозам ИБ. Однако, их использование не всегда экономически оправданно, из-за сложности эксплуатации и высокой стоимости. Для защиты автономных автоматизированных рабочих мест (АРМ) экономически и технически более целесообразно использовать менее сложные и дорогостоящие решения и средства. В данной статье дана краткая характеристика достоинств и недостатков современных USB-устройств, проанализированы связанные с их применением потенциальные угрозы ИБ и способы противодействия им. Описаны состав, структура и алгоритмы функционирования программного комплекса управления доступом USB-устройств, предназначенного для защиты автономных автоматизированных рабочих мест, функционирующих под управлением операционной системы Windows.

1. Анализ характеристик и возможностей USB-устройств

USB-интерфейс (Universal Serial Bus – универсальная последовательная шина) – это последовательный интерфейс передачи данных для периферийных устройств в вычислительной технике. В настоящее время интерфейс USB (спецификации версий от 2.0 до 3.2) является основным коммуникационным протоколом для подключения и обмена данными с компьютерами таких устройств, как мыши, клавиатуры, принтеры, сканеры, модемы, кардридеры, флэш-накопители, фотоаппараты, сотовые телефоны, плееры, жёсткие диски, оптические дисководы и др. [1]. USB-интерфейс практически полностью заменил другие интерфейсы: COM-порт – для мыши, PS/2 – для клавиатуры, параллельный порт – для принтера. Это обусловлено следующими его характеристиками и возможностями[6].

1. Универсальностью и распространенностью. Все современные компьютеры оснащены несколькими портами USB (на современных настольных ПК их до 12, на большинстве ноутбуков от 2-х до 4-х). USB используют такие устройства, как фото и видеокамеры, клавиатуры, принтеры и другие периферийные устройства.

2. Простота в использовании. USB-устройства можно подключать и отключать во время работы компьютера (Plug and Play). Современные операционные системы сразу же распознают USB-устройства и подгружают необходимые драйверы.

3. Высокая пропускная способность. Для интерфейса USB 2.0 она составляет 480 Мбит/с. Копирование файла размером 700 Мб на накопитель, подключенный к порту USB 2.0, займет не более 20 секунд. В стандарте USB 3.0 пропускная способность достигла уровня 5 Гбит/с, в версии USB 3.2 (SuperSpeed USB 20Gbps) – до 20 Гбит/с[7], в новой версии USB 4.0 возрастет до 40 Гбит/с[8].

4. Обеспечение питания. Порт USB не только служит для подключения периферии, но и может подавать питание на устройства с низким энергопотреблением: мыши, клавиатуры, съемные USB-флеш-носители и внешние жесткие диски.

Широкое распространение и активное использование USB-накопителей, практически вытеснивших все другие переносные средства хранения данных, обусловлены следующими свойствами этих устройств[9]:

- компактностью – при минимальных размерах флешки позволяют хранить до 256 ГБ данных;
- универсальностью – подключение через один USB-порт проще, чем через два, как того требуют быстрые внешние винчестеры, и точно проще, чем использование карт-ридера;
- экономичностью – флеш-память имеет одно из лучших соотношений цена/объём данных;
- надёжностью – флешки в герметичном ударопрочном корпусе, не боятся ни воды, ни падения с высоты, пыли и механических вибраций за счёт отсутствия движущихся частей.
- К числу недостатков флешек относятся:
- невысокая износоустойчивость при частой эксплуатации;
- чувствительность к электромагнитному импульсу;
- криптографическая ненадёжность;
- легкость потери, кражи, подмены, бесконтрольного выноса за пределы контролируемой зоны.

Активное использование USB-устройств в государственных и корпоративных информационных системах, обусловленное их преимуществами перед другими средствами хранения информации, имеет и не-

5 http://www.infowatch.ru/analytics

6 https://www.ixbt.com/data/sandisk-extreme-go-pro-review.html

7 https://www.usb.org/superspeed-usb

8 https://habr.com/ru/news/t/466269/

9 https://www.anti-malware.ru/analytics/Threats_Analysis/security-flaws-in-usb

гативную сторону – USB-устройства стали одними из наиболее опасных и активно используемых средств и каналов реализации угроз ИБ.

2. Анализ уязвимостей и угроз информационной безопасности, связанных с использованием USB-устройств

Спецификация интерфейса USB изначально разрабатывалась без учета вопросов обеспечения информационной безопасности систем, которые будут использовать USB-устройства. Приоритетными при создании технологии USB были такие свойства как гибкость, универсальность, простота и удобство использования. Для обеспечения этого каждое устройство USB имеет собственный чип контроллера и память для прошивки программной реализации специфичных для него функций. Все USB-устройства взаимодействуют с операционной системой через универсальный USB-контроллер, который определяет класс USB-устройства и сообщает его операционной системе. После этого происходит установка драйверов и с устройством становится возможным взаимодействовать.

При этом операционные системы (Windows, Linux, macOS) доверяют любому подключенному к порту USB-устройству. Когда USB-устройство подключается к компьютеру, чип выполняет код прошивки. На легитимном накопителе прошивка запрограммирована на то, чтобы зарегистрировать себя в качестве устройства и загрузить драйвер, который впоследствии будет установлен. Прошивку можно запрограммировать так, что обычная USB флэшка будет рассматриваться, как клавиатура или сетевой адаптер, что позволит злоумышленнику реализовать различные виды атак вплоть до получения полного контроля над системой. Используя данную уязвимость, получившую название BadUSB, можно реализовать следующие атаки [2 – 5].

1. Подключенный к системе USB флеш-накопитель с перепрошитой памятью может выдать себя за клавиатуру и начать отдавать команды от имени пользователя, под которым был выполнен вход в ОС. Если был выполнен вход от имени администратора, устройство получает полный доступ ко всем возможностям ОС.

2. USB-устройство с BadUSB уязвимостью может эмулировать сетевую карту компьютера, с помощью специальной прошивки осуществить подмену стандартных DNS-адресов и перенаправить весь трафик через подставной сервер, получив возможность совершать атаку типа «человек посередине».

3. USB-накопитель, который будет использован для переустановки ОС, может уже быть заражен BadUSB-инфекцией и сразу, при установке, прописать в памяти компьютера вредоносные файлы и заразить «чистую» ОС. Администратор может и не узнать об этом, потому что вредоносные файлы будут находиться уже в самой ОС до установки антивирусной программы.

4. USB-устройства с установленными в них специальными программами могут осуществлять сокрытие вредоносных файлов от средств защиты ОС и антивирусов, например посредством модифицирования зараженных файлов «на лету». Антивирусная программа проверяет «чистый» файл до его изменения, после этого на USB-накопитель записывается зараженный файл.

Спектр возможных атак с помощью USB-устройств ограничен только возможностями и целями нарушителей. Описание различных вариантов атак, реализуемых с помощью USB- устройств, представлены также в статьях [6 – 13]. Учитывая тот факт, что атаки реализуются на уровне микрокодов, опасность и универсальность их реализации очень высоки. В следующем разделе представлен обзор методов и средств, используемых для защиты от этих угроз.

3. Обзор методов и средств защиты от угроз информационной безопасности, реализуемых посредством USB-устройств

Для противодействия угрозам ИБ, реализуемых посредством USB-устройств, используются два подхода. Первый подход предполагает полный запрет и отключение физической возможности использования USB-устройств. Второй подход основан на использовании программных и аппаратно-программных СЗИ НСД и реализации соответствующих организационно-технических мер. Полный запрет и отключение физической возможности использования USB-устройств можно осуществить следующими способами[10]:

- отключить USB через настройки BIOS;
- изменить параметры реестра для USB-устройств;
- отключить USB-порты в диспетчере устройств;
- деинсталлировать драйверы контроллера USB;
- использовать дополнительные программы;
- осуществить физическое отключение USB-портов.

При реализации второго подхода, предусматривающего регулируемое и контролируемое использование USB-устройств, используются следующие классы СЗИ:

- программные и программно-аппаратные СЗИ НСД: «Dallas Lock», «Secret Net», «Аккорд», «DeviceLock DLP» и др.;
- средства предотвращения утечек конфиденциальной информации за пределы защищаемой сети – DLP-системы (Data Leak Prevention): «SecurIT ZGate», «InfoWatch Traffic Monitor», «Symantec Data Loss Prevention», «Search Inform Контур безопасности», «FalconGaze SecureTower» и др.;
- средства криптографической защиты информации (СКЗИ) или IRM-системы (Information Rights Management): «Adobe LiveCycle Rights Management», «Check Point Document Security», «EMC Documentum IRM Services», «Microsoft AD RMS», «Oracle IRM» и др.

Применение возможностей СЗИ НСД является более предпочтительным решением с точки зрения надежности и управления, поскольку оно позволяет использовать единый центр управления, единую систему аутентификации и авторизации пользователей, обеспечивает аппаратную поддержку защиты и способно контролировать доступ к разнообразным интерфейсам,

10 https://sysadmin.ru/articles/zapretit-ispolzovanie-USB-fleshnakopitelej-fleshek-na-kompyutere

не только к USB. В отличие от мер, полностью блокирующих использование USB-устройств, они позволяют делать это более точно и конкретно с учетом особенностей систем и ролей пользователей. С помощью интегрированной консоли управления определяется каким пользователям предоставить доступ к тем или иным локальным портам, на каких компьютерах, в какое время, для каких операций (чтение, запись, выполнение) и т.п. В то же время применение столь мощных СЗИ НСД имеет следующие ограничения и недостатки: высокая стоимость продукта, большое потребление ресурсов персональных компьютеров, не всегда самых быстродействующих, сложность обучения, трудоемкость конфигурирования, что часто обуславливает неполное использование возможностей этих систем для предотвращения утечек информации.

Следующий класс СЗИ – системы сегмента DLP [14 – 17]. Главной их характеристикой является глубокий анализ информационного содержимого исходящих данных. Подобные решения определяют легитимность той или иной операции на базе технологий глубокой контентной фильтрации. Однако уровень качества их современной реализации пока не позволяет обеспечить необходимый уровень полноты и точности контроля информации, передающейся по локальным портам на мобильные носители. Это обусловлено следующими причинами[11].

Во-первых, современный уровень технологии контентной фильтрации не позволяет полностью избежать ошибок ложного распознавания содержимого данных — так называемых ложноположительных и ложноотрицательных срабатываний. В существующих системах уровень точности контентной фильтрации редко превышает 80-85% .

Во-вторых, глубокий контентный анализ — весьма ресурсоемкий процесс. Когда отправляется письмо по электронной почте, DLP-система перехватывает его в сети и анализирует на уровне SMTP-сервера с достаточной для этой задачи производительностью. Если же информация копируется локально, такой подход неприменим, поскольку информация в принципе не попадает в сеть. В результате приходится идти на компромисс: либо пересылать теневые копии информации на сервер и потом получать по ней вердикт, либо анализировать информацию локально. В первом случае создается значительная нагрузка на сеть, что может привести к длительным задержкам (например, при копировании на съемный носитель видео файлов), а во втором — страдает качество анализа, поскольку персональному компьютеру не хватает мощности для данного вида обработки, либо он работает по более простым и менее надежным алгоритмам.

Третья причина, ограничивающая применение DLP-систем для контроля локальных портов, тесно связана с первой. Дело в том, что DLP-системы изначально были спроектированы как шлюзовые решения для анализа сетевого трафика, поэтому их агентские компоненты еще не достигли уровня, необходимого для контроля других интерфейсов, в частности USB портов. Кроме того, требуются дополнительные усилия по встраиванию DLP-систем в единую систему обеспечения ИБ. Сами эти системы не обеспечивают безопасность вычислительной среды, а потому для их безопасного функционирования требуется установка тех же СЗИ НСД.

Таким образом, использование DLP-систем для контроля доступа пользователей к USB-носителям оправданно в двух случаях. Во-первых, когда эти средства не столь обременительны по цене, как СЗИ НСД, а использование последних не является необходимым. Это системы с нарушителем класса не выше Н2 по классификации ФСТЭК. Во-вторых, использование для расширения функционала СЗИ НСД в том случае, когда доказана работоспособность этого расширенного функционала.

Средства криптографической защиты информации или системы класса IRM не ограничивают использование USB-устройств, однако могут существенно снизить возникающие при их использовании риски нарушения ИБ. Работа типичной IRM-системы строится на базе двух механизмов: меток конфиденциальности и шифрования. Каждый защищаемый файл помещается в шифрованный контейнер вместе со специальной меткой, определяющей права доступа к нему. Если такой контейнер будет похищен или утерян, то без знания секретной информации о ключах шифрования доступ к хранящейся в нем информации будет закрыт. С точки зрения контроля информации, перемещаемой на съемных носителях, данная схема практически эквивалентна принудительному шифрованию экспортируемых на съемные носители данных, которое часто встречается в системах контроля доступа к портам и периферийным устройствам. Системы класса IRM разрешают экспорт конфиденциальной информации только в зашифрованном виде, что позволяет всегда защитить организацию от случайных утечек, но редко от утечек спланированных. Производительность IRM-систем существенно зависит от количества «защищаемых» файлов и интенсивности их модификаций пользователем. Для больших систем и высокой динамике изменения данных их использование потребует значительных вычислительных ресурсов. Ограничивающим фактором применения систем данного класса также является относительно высокая сложность управления средствами криптографической защиты информации, включая подсистему генерации и хранения ключей шифрования.

Каждый способ защиты от угроз, связанных с использование USB-устройств, представляет собой компромисс между удобством пользователей, требованиями службы безопасности и стоимостью системы. Современные DLP-системы контентной фильтрации пока не могут полностью решить проблему локальных утечек данных с компьютеров сотрудников организации. На современной стадии развития средств защиты от инсайдерских утечек иногда более эффективным является использование простых, но при этом гораздо более дешевых и надежных средств разграничения доступа, обладающих возможностями контекстного контроля в сочетании с некоторым базовым функционалом фильтрации контента.

11 https://www.anti-malware.ru/analytics/Market_Analysis/Discovery-DLP

В качестве подобного решения эконом-класса предлагается использовать программный комплекс управления доступом USB-устройств к защищаемому АРМ, обеспечивающий обнаружение подключаемых устройств, проверку их легитимности по защищенной базе разрешенных USB-устройств, блокировку нелегитимных подключений, регистрацию связанных с этими операциями событий. В следующем разделе представлено описание состава, структуры и алгоритмов функционирования такого программного средства.

4. Состав и алгоритмы функционирования программного комплекса управления доступом USB-устройств к защищаемым ресурсам

Программный комплекс управления доступом USB-устройств (ПК УД-USB) предназначен для защиты АРМ, функционирующих под управлением операционной системы MS Windows, от угроз ИБ, реализуемых посредством USB-устройств. ПК УД-USB обеспечивает:

- создание и ведение базы данных USB устройств, разрешенных для использования на данном АРМ (БД USB);
- обнаружение и проверку легитимности использования USB-устройств по БД USB;
- автоматическое извлечения (отключение) не прошедших проверку устройств;
- регистрацию информации о фактах подключения и способах использования USB устройств в доступный только администратору по безопасности зашифрованный log-файл.

Программный комплекс состоит из двух основных программ: StopFlashAccess и StopFlashGuard. Первая предназначена для создания и ведения БД USB. Вторая реализует основной функционал ПК. Программы разработаны в интегрированной среде разработки ПО Microsoft Visual Studio 2010 на языке программирования C++ с использованием технологий WinAPI и Windows Forms.

Программа StopFlashAcess предназначена для управления зашифрованной базой данных учтенных носителей и выполняет следующие функции:

- ввод логина и пароля (с возможностью изменения) для входа в программу;
- приостановка и возобновление работы StopFlashGuard для исключения конфликтов доступа к общей базе данных;
- контроль наличия и целостности файла базы учтенных устройств;
- просмотр базы данных;
- просмотр log-файла учета манипуляций с базой данных и USB-устройствами;
- просмотр статистики использования USB-носителей;
- ввод серийного номера и типа устройства в имеющуюся базу данных;
- ввод информации о владельце USB-носителя (ФИО, должность, подразделение и др.) в базу данных;
- сканирование USB-портов на наличие подключенных устройств и, при необходимости, добавление информации о них (серийный номер, производитель, наименование, тип) в базу данных;
- запись в служебную область USB-носителя шифрованной учетной информации об устройстве и его владельце с целью идентификации в случае подмены серийного номера;
- удаление учетной записи о USB-устройстве из базы данных;
- хранение актуальной базы данных и log-файла в зашифрованном виде;
- загрузка из текстового файла новой базы данных;
- добавление из текстового файла информации об USB-устройствах к имеющейся базе данных;
- сохранение актуальной базы данных в текстовый файл;
- сохранение log-файла в текстовый файл.

Для шифрования файлов был применен алгоритм ГОСТ 28147, который является отечественным стандартом симметричного блочного шифрования (длина блока – 64 бита, длина ключа – 256 битов, количество раундов – 32, применены S-boxes, используемые в приложениях Центрального Банка РФ) [18, 19]. Поточное шифрование проведено в режиме CBC (Cipher Block Chaining), когда вход криптографического алгоритма является результатом применения операции XOR (eXclucive OR) к следующему блоку незашифрованного текста и предыдущему блоку зашифрованного текста.

Программа StopFlashGuard запускается при загрузке операционной системы и может функционировать в одном из трех режимах: демонстрации, защиты и наблюдения.

Демонстрационный режим используется для отладки, визуального наблюдения и анализа хода и результатов работы программы. Все контролируемые ПК события фиксируются в log-файле программы и выводятся на экран.

Основным является режим защиты, в котором выполняется обнаружение и автоматическое извлечение (логическое отключение) не прошедших проверку USB-устройств. Пользователь получает только сообщения об отключении нелегитимного устройства. Информация об этом также записывается в log-файл программы.

Режим наблюдения предназначен для обнаружения фактов использования нелегитимных USB-устройств, отслеживания и регистрации выполненных с помощью данного устройства операций, а также последующего анализа собранной информации. Отключение нелегитимных USB не производится, пользователь о фиксируемых ПК событиях не информируется.

Тип режима функционирования программы StopFlashGuard задается с помощью параметра командной сроки: demo – для демонстрационного, transparent – для режима наблюдения. По умолчанию программа выполняется в режиме защиты.

Обобщённый алгоритм работы программы StopFlashGuard представлен на рис. 1 и рис.2. На рис. 1 представлена схема алгоритма главной функции программы StopFlashGuard – _tWinMain(). На рис. 2 представлена схема алгоритма функции WndProc(), которая реализует функционал программного комплекса.

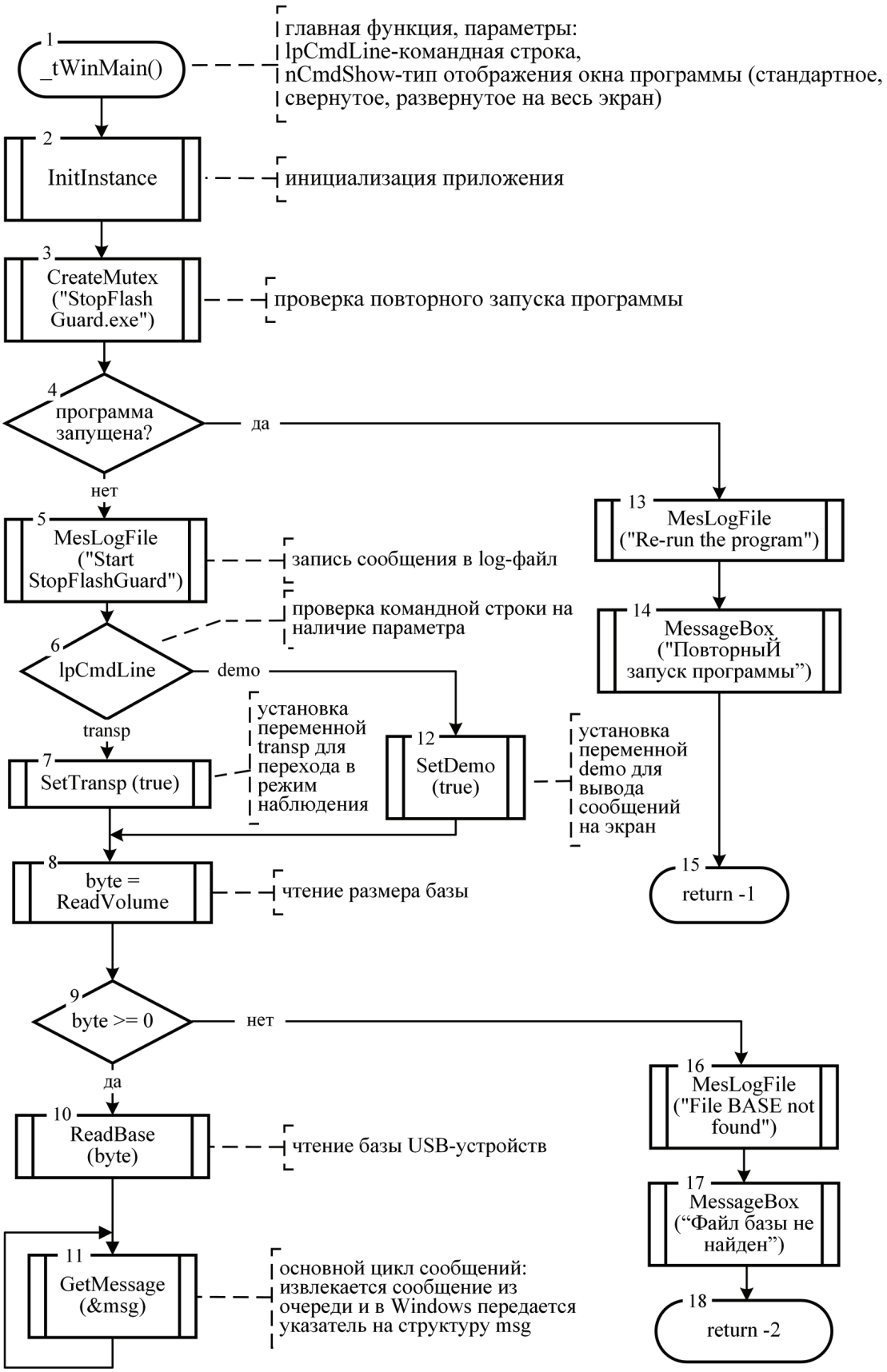

Рис.1. Алгоритм главной функции _tWinMain() программы StopFlashGuard

DOI:10.21681/2311-3456-2020-01-52-61

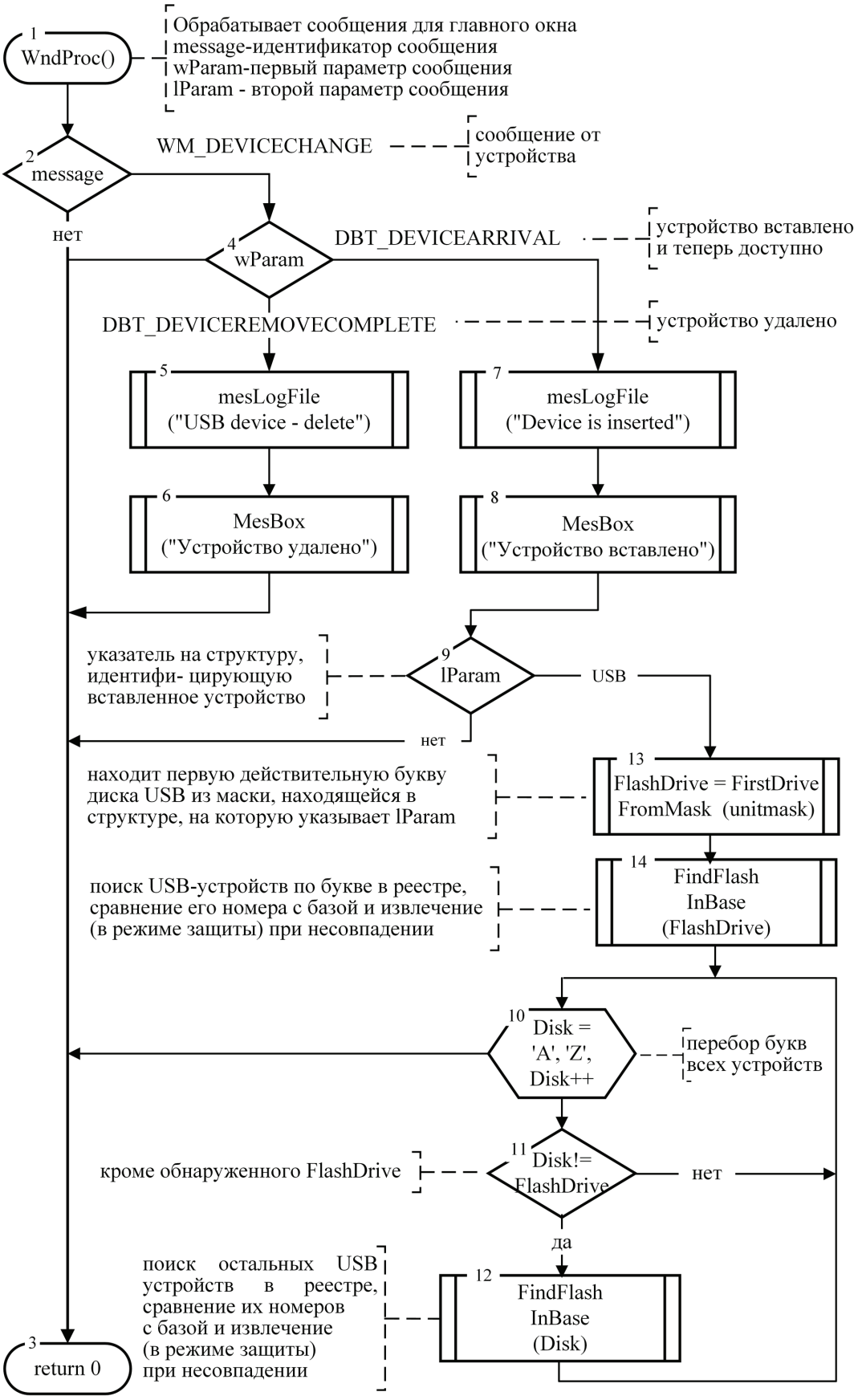

Рис. 2. Алгоритм функции WndProc() программы StopFlashGuard

В соответствии с представленными на рис.1 и рис.2 схемами программа StopFlashGuard выполняет следующую последовательность операций:

- проверку и предотвращение повторного запуска программы (блоки 3-4, 13-15 рис.1);
- определение по параметру командной строки режима работы ПК и его инициализацию (блоки 6-7, 12 рис.1);
- контроль наличия и целостности БД USB (блоки 8-10, 16-18 рис.1);
- обнаружение подключаемых к USB-портам устройств (блок 11 рис.1, блоки 1-9 рис.2);
- поиск в БД USB информации о вновь подключенном устройстве (наименование, производитель, серийный номер, тип) (блоки 10-14 рис.2);
- проверку соответствия контролируемых атрибутов подключенного USB-устройства (устройств) с информацией из БД USB (блоки 12,14 рис.2);
- автоматическое извлечение (логическое отключение) неучтенных устройств в режиме защиты (блоки 12,14 рис.2);
- обнаружение изъятия носителей из USB-порта (блоки 4-6 рис.2);
- регистрацию всех манипуляций с USB-носителями в log-файле ПК.

Результаты испытаний ПК УД-USB подтвердили его функциональную пригодность для реализации эффективного контроля использования USB-устройств на автономных АРМ, продемонстрировали простоту и удобство настройки и применения. Основными направлениями дальнейшего развития ПК УД-USB являются:

- контроль двунаправленного копирования, перемещения, удаления файлов и запуска программ с возможностью блокировки или только однонаправленной передачи информации;
- реализация сетевого варианта программного комплекса по технологии клиент-сервер с размещением БД USB на сервере информационной безопасности, а клиентских приложений на АРМ защищаемой сети;
- портирование комплекса на операционные системы, основанные на ядре Linux;
- применение радиочастотной идентификации RFID (Radio Frequency IDentification) для предотвращения выноса за пределы территории учреждения недобросовестными сотрудниками учтенных носителей информации;
- разработка внешнего компактного (или встроенного в ПК) аппаратного блока защиты (переходника) на базе микроконтроллера STM32 с ЦПУ ARM Cortex-M3, реализующего покластерное шифрование носителя (с целью предотвращения доступа к информации за пределами организации) и другие функции защиты.

Выводы

Тенденция все более активного использования для хранения и обмена информацией USB-устройств в ближайшем будущем не только сохранится, но и получит новые импульсы[12]. Это обусловлено постоянным совершенствованием и развитием данной технологии, расширенным производством все новых и новых систем и устройств, построенных на ее основе[13] [20 – 21]. При этом очевидно и то, что также активно будут развиваться и совершенствоваться методы и средства реализации с их помощью атак на критически важные автоматизированные системы управления и информационные ресурсы.

Представленный в данной статье ПК управления доступом USB-устройств относится к решениям эконом-класса и обеспечивает необходимый уровень защиты автономных АРМ, функционирующих под управлением ОС Windows, посредством обнаружения подключаемых устройств, проверки их легитимности по защищенной базе данных о разрешенных USB-устройствах, блокировки нелегитимных подключений, регистрации связанных с этими операциями событий. Кроме того, данный ПК может использоваться для обнаружения фактов нелегитимного использования USB-устройств, отслеживания и регистрации выполненных с их помощью операций для выявления и анализа инсайдерской деятельности. Основными направлениями совершенствования ПК являются: расширение его функциональных возможностей с учетом развития данной технологии и реализации USB-устройств, появления новых угроз, а также портирование на другие аппаратно-программные платформы и разработка аппаратной реализации.

Рецензент: *Езерский Владимир Васильевич, доктор технических наук, профессор, заместитель генерального директора по науке и развитию, Акционерное общество «Научно-исследовательский институт программных средств», Санкт-Петербург, Россия. E-mail:office@nii-ps.ru.*

12 https://www.usb.org/

13 http://vention.su/index.php?route=simple_blog/article/view&simple_blog_article_id=22.

Литература

1. USB Complete: The Developer's Guide (Complete Guides series) Fifth Edition, Fifth edition. Edition by Jan Axelson. Published by Lakeview Research LLC, March 1, 2015. 524p.
2. Полежаев П.Н., Малахов А.К., Сагитов А.М. «Ахиллесова пята» USB-устройств: атака и защита // Философские проблемы информационных технологий и киберпространства. 2015. № 1(9). С. 106–117. DOI: 10.17726/philIT.2015.9.1.4.491.
3. Nir Nissim, Ran Yahalom, Yuval Elovici: USB-based attacks, in Computers & Security, vol. 70, pp. 675-688, 2017.
4. Abhijeet Ramani, Somesh Kumar Dewangan: Auditing Windows 7 Registry Keys to track the traces left out in copying files from system to external USB Device" in International Journal of Computer Science and Information Technologies, vol. 5 ,2, pp.1045-1052, 2014.
5. Angel, S., Wahby, R.S., Howald, M., Leners, J.B., Spilo, M., Sun, Z., Blumberg, A.J., Walfish, M.: Defending against malicious peripherals with Cinch. In: USENIX Security Symposium (2016).
6. Francisco Ramírez Pablo González Carmen Torrano José María Alonso. Discovering and Plotting Hidden Networks created with USB Devices. CDO, Telefónica Madrid, Spain. https://www.exploit-db.com/docs/english/44947-discovering-and-plotting-hidden-networks-created-with-USB-devices.pdf?rss
7. A.Crenshaw. Plug and Prey: Malicious USB devices. In Proceedings of ShmooCon, Jan. 2011.
8. J. Maskiewicz, B. Ellis, J. Mouradian, and H. Shacham. Mouse trap: Exploiting firmware updates in USB peripherals. In Proceedings of the USENIX Workshop on Offensive Technologies, Aug. 2014.
9. Вахний Т.В., Кузьмин С.Ю. Разработка аппаратно-программного средства защиты от уязвимости BadUSB. Математические структуры и моделирование 2016. №2(38). С. 116–125.
10. Thunderclap: Exploring Vulnerabilities in Operating System IOMMU Protection via DMA from Untrustworthy Peripherals. Network and Distributed Systems Security (NDSS) Symposium 2019 24-27 February 2019, San Diego, CA, USA ISBN 1-891562-55-X https://dx.doi.org/10.14722/ndss.2019.23194 www.ndss-symposium.org
11. S. Gallagher, "New WikiLeaks dump: The CIA built Thunderbolt exploit, implants to target Macs," Mar. 2017. [Online]. Available: https://arstechnica.com/security/2017/03/new-wikileaks-dump-the-ciabuilt-thunderbolt-exploit-implants-to-target-macs.
12. USBlock: Blocking USB-Based Keypress Injection Attacks: 32nd Annual IFIP WG 11.3 Conference, DBSec 2018, Bergamo, Italy, July 16–18, 2018, Proceedings.
13. Tian, Dave & Bates, Adam & Butler, Kevin. (2015). Defending Against Malicious USB Firmware with GoodUSB. 261-270. 10.1145/2818000.2818040.
14. Обзор DLP-системы InfoWatch Traffic Monitor 6.7 https://www.anti-malware.ru/reviews/infowatch-traffic-monitor-6-7.
15. Overview of data loss prevention. https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies.
16. Best data loss prevention service of 2019: Choose the right DLP to protect your assets. https://www.techradar.com/best/best-data-loss-prevention-service.
17. López G., Richardson N.; Carvajal J. Methodology for Data Loss Prevention Technology Evaluation for Protecting Sensitive Information. Revista Politécnica – Septiembre 2015, Vol. 36, No. 3.
18. Фергюсон Н. Шнайер Б. Практическая криптография. М.: Издательский дом «Вильямс». 2005. 424 с.
19. Э. М. Габидулин, А. С. Кшевецкий, А. И. Колыбельников. «Защита информации: учебное пособие». М.: МФТИ, 2011. 262 с. ISBN 5-7417-0377-9.
20. Apple and Microsoft are both making a big bet on the future of USB. https://www.businessinsider.com/apple-microsoft-surface-USB-c-2018-10.
21. USB flash drive market report.http://thescrippsvoice.com/market-research-news/154618/USB-flash-drive-market-report-a-complete-overview-of-market-segments-and-the-regional-outlook-of-usb-flash-drive-industry.

THE SOFTWARE COMPLEX ACCESS CONTROL USB DEVICES TO AUTOMATED WORKSTATIONS

Baev A.V.[14], Gacenko O.U.[15], Samonov A.V.[16]

Abstract: *Currently, to connect to computers any external devices, starting with flash drives, photo and video cameras and ending with office equipment and sophisticated medical devices, more and more actively used serial USB data interface. The wide use of USB devices for data storage and transmission is due to their versatility, reliability, performance, simplicity and convenience. At the same time, USB devices are one of the most dangerous and actively used tools and channels for implementing information security threats.*

14 Aleksey Baev, senior researcher, Military space Academy A.F.Mozhaisky, Saint-Petersburg, Russia, E-mail: baih@mail.ru

15 Oleg Gacenko, Dr.Sc, AO NII PS, Saint-Petersburg, Russia, E-mail: gatsen@mail.ru

16 Aleksandr Samonov, Ph.D, senior researcher, Military space Academy A.F.Mozhaisky, Saint-Petersburg, Russia, E-mail: a.samonov@mail.ru

The purpose of the study, the results of which are presented in this article, is to increase the security of autonomous automated workplaces from threats to information security implemented with the help of USB-devices.

Research methods: *to achieve this goal, the technical characteristics and functionality of USB-devices were investigated, the potential vulnerabilities and ways of their operation for the implementation of information security threats were identified, and the advantages and disadvantages of existing approaches and means of protection were analyzed.*

The result of research and work: *created software complex for access control of USB-devices, which provides protection of autonomous automated workplaces operating under Windows OS by detecting connected devices, checking their legitimacy on a secure database of allowed USB-devices, blocking illegitimate connections, registering events associated with these operations. This software complex can also be used to detect the facts of illegal use of USB-devices, tracking and recording operations performed with their help to identify and analyze insider activity. The description of the composition, structure and functioning algorithms of this software complex is given. The main directions of its development and improvement are defined.*

Keywords: *access control, information security threats, security algorithms and tools, USB devices, USB vulnerabilities*

References

1. USB Complete: The Developer's Guide (Complete Guides series) Fifth Edition, Fifth edition. Edition by Jan Axelson. Published by Lakeview Research LLC, March 1, 2015. 524p.
2. Polezhaev P.N., Malahov A.K., Sagitov A.M. «Ahillesova pyata» USB-ustrojstv: ataka i zashchita // Filosofskie problemy informacionnyh tekhnologij i kiber-prostranstva. 2015. № 1(9). C. 106–117.
3. Nir Nissim, Ran Yahalom, Yuval Elovici: USB-based attacks, in Computers & Security, vol. 70, pp. 675-688, 2017.
4. Abhijeet Ramani, Somesh Kumar Dewangan: Auditing Windows 7 Registry Keys to track the traces left out in copying files from system to external USB Device" in International Journal of Computer Science and Information Technologies, vol. 5 ,2, pp.1045-1052, 2014.
5. Angel, S., Wahby, R.S., Howald, M., Leners, J.B., Spilo, M., Sun, Z., Blumberg, A.J., Walfish, M.: Defending against malicious peripherals with Cinch. In: USENIX Security Symposium (2016).
6. Francisco Ramírez Pablo González Carmen Torrano José María Alonso. Discovering and Plotting Hidden Networks created with USB Devices. CDO, Telefónica Madrid, Spain. https://www.exploit-db.com/docs/english/44947-discovering-and-plotting-hidden-networks-created-with-usb-devices.pdf?rss
7. A.Crenshaw. Plug and Prey: Malicious USB devices. In Proceedings of ShmooCon, Jan. 2011.
8. J. Maskiewicz, B. Ellis, J. Mouradian, and H. Shacham. Mouse trap: Exploiting firmware updates in USB peripherals. In Proceedings of the USENIX Workshop on Offensive Technologies, Aug. 2014.
9. T.V. Vahnij, S.YU. Kuz'min. Razrabotka apparatno-programmnogo sredstva zashchity ot uyazvimosti BadUSB. Matematicheskie struktury i modelirovanie 2016. №2(38). S. 116–125.
10. Thunderclap: Exploring Vulnerabilities in Operating System IOMMU Protection via DMA from Untrustworthy Peripherals. Network and Distributed Systems Security (NDSS) Symposium 2019 24-27 February 2019, San Diego, CA, USA ISBN 1-891562-55-X https://dx.doi.org/10.14722/ndss.2019.23194 www.ndss-symposium.org
11. S. Gallagher, "New WikiLeaks dump: The CIA built Thunderbolt exploit, implants to target Macs," Mar. 2017. [Online]. Available: https://arstechnica.com/security/2017/03/new-wikileaks-dump-the-ciabuilt-thunderbolt-exploit-implants-to-target-macs.
12. USBlock: Blocking USB-Based Keypress Injection Attacks: 32nd Annual IFIP WG 11.3 Conference, DBSec 2018, Bergamo, Italy, July 16–18, 2018, Proceedings.
13. Tian, Dave & Bates, Adam & Butler, Kevin. (2015). Defending Against Malicious USB Firmware with GoodUSB. 261-270. 10.1145/2818000.2818040.
14. Obzor DLP-sistemy InfoWatch Traffic Monitor 6.7 https://www.anti-malware.ru/reviews/infowatch-traffic-monitor-6-7.
15. Overview of data loss prevention. https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies.
16. Best data loss prevention service of 2019: Choose the right DLP to protect your assets. https://www.techradar.com/best/best-data-loss-prevention-service.
17. López G., Richardson N.; Carvajal J. Methodology for Data Loss Prevention Technology Evaluation for Protecting Sensitive Information. Revista Politécnica – Septiembre 2015, Vol. 36, No. 3.
18. Фергюсон Н. Шнайер Б. Практическая криптография. – М.: Издательский дом «Вильямс». 2005. – 424 с.
19. Э. М. Габидулин, А. С. Кшевецкий, А. И. Колыбельников. «Защита информации: учебное пособие». – М.: МФТИ, 2011. – 262 с. – ISBN 5-7417-0377-9.
20. Apple and Microsoft are both making a big bet on the future of USB. https://www.businessinsider.com/apple-microsoft-surface-usb-c-2018-10.
21. USB flash drive market report.http://thescrippsvoice.com/market-research-news/154618/usb-flash-drive-market-report-a-complete-overview-of-market-segments-and-the-regional-outlook-of-usb-flash-drive-industry.