КАТАЛОГ ЗАКЛАДОК АНБ (SPIGEL). ЧАСТЬ 2. РАБОЧЕЕ МЕСТО ОПЕРАТОРА

Клянчин Александр Иванович

Представлено продолжение анализа закладки по версии журнала Spiegel [1]. Обоснована теоретическая база программно–аппаратных закладок. Приведено описание закладок, возможность встраивания, вероятное применения.

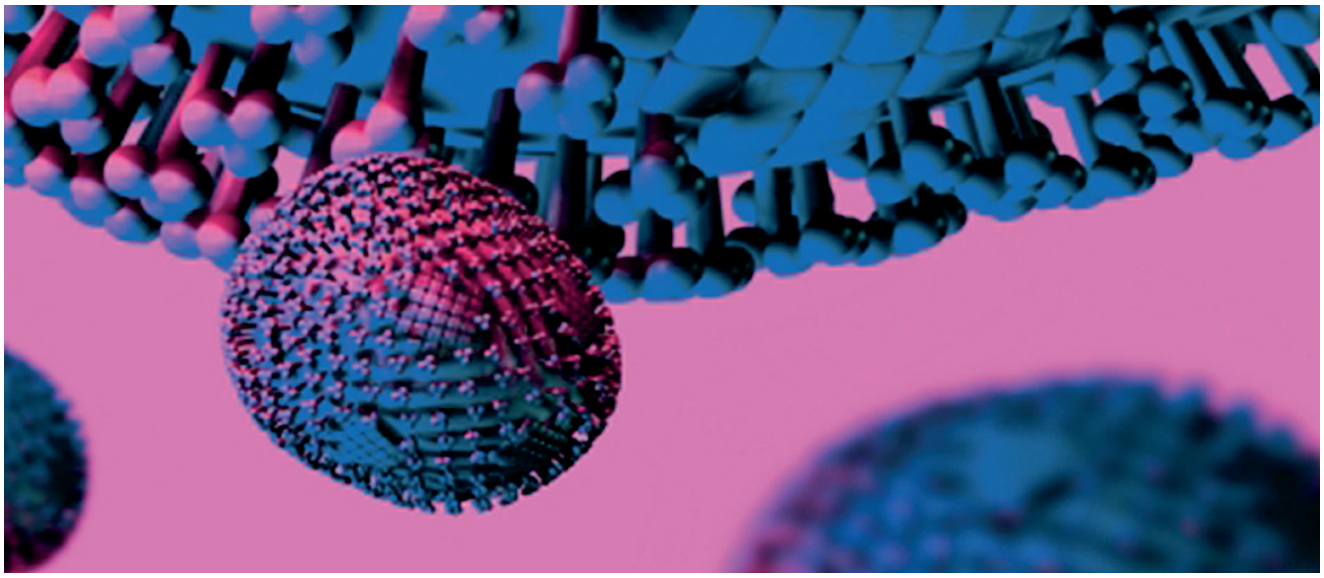
***Ключевые слова**: программные и аппаратные закладки, уязвимость аппаратной платформы, механизмы безопасности, кибербезопасность, кибероружие.*

THE NSA'S SPY CATALOG. PART 2. OPERATOR'S WORKPLACE

Alexander Klyanchin

The infrastructure NSA implants (reviewed in Spiegel) are considered [1]. The theory of the hardware and software are shown. There are descriptions, implanting features, application of the implants.

***Keywords**: software implant, hardware implant, hardware vulnerability, security controls, information security management, cybersecurity, cyber weapons.*



Введение

В данной статье мы продолжаем анализ закладок, упоминаемых в журнале Spiegel [1].

Структурно средства автоматизации организации можно разделить на две части:

1. **Инфраструктурные средства**, к которым относятся: подключения к внешним каналам, локальные вычислительные сети, организация беспроводного доступа, сервера и др.
2. **Оборудование пользовательских рабочих мест**, к которым относятся: рабочая станция, сотовая связь и др.

Данное деление также используется при выработке решений встраивания зловредных закладок. При этом учитывается степень доступности данных устройств для доработок, а также уровень и область компетентности цели для каждого потенциального канала утечки. Например, потенциальная угроза общей организации работ может быть нанесена путем контроля инфраструктуры компании, а потенциальная угроза определенной области деятельности может быть нанесена при атаке на конкретного исполнителя и его рабочее место.

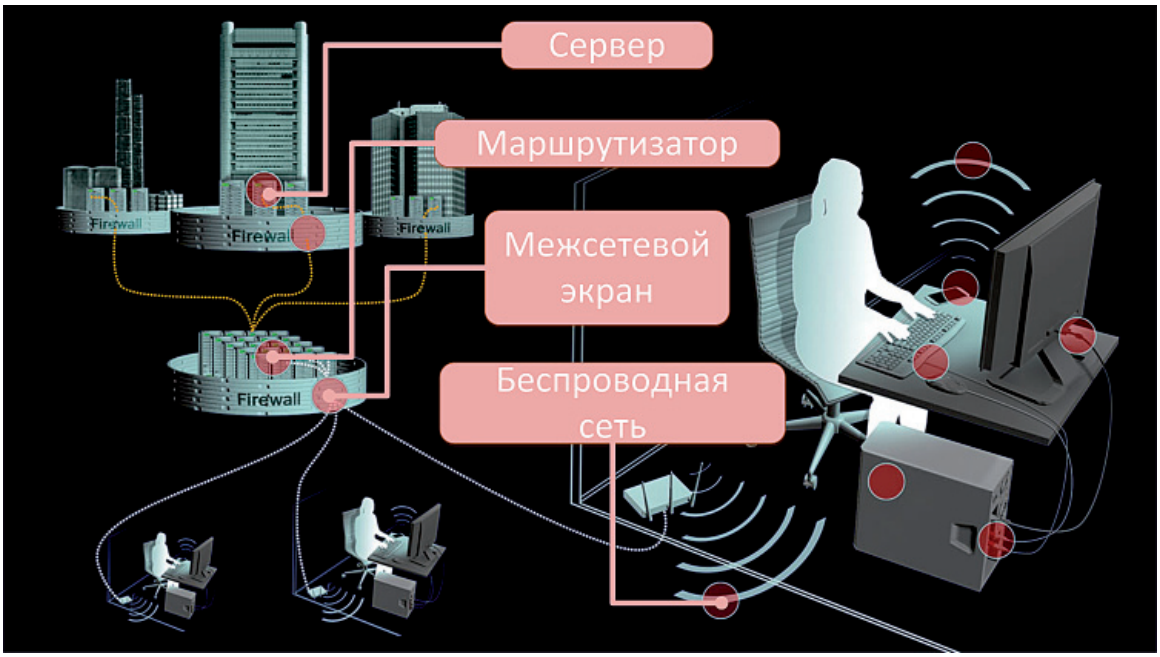


Рис. 2. *Потенциальная возможность установки закладок на элементы инфраструктуры*

В первой части обзора статьи «Каталог закладок АНБ (Spigel)» были представлены программно-аппаратные закладки, ориентированные на инфраструктуру организации (см. Рис. 1). В рамках данной статьи предлагается рассмотреть потенциальные способы использования закладок на уровне пользователя (см. Рис. 2. Потенциальная возможность установки закладок на оборудование рабочего места пользователя), а также продемонстрировать возможные сценарии использования по версии журнала Spiegel.

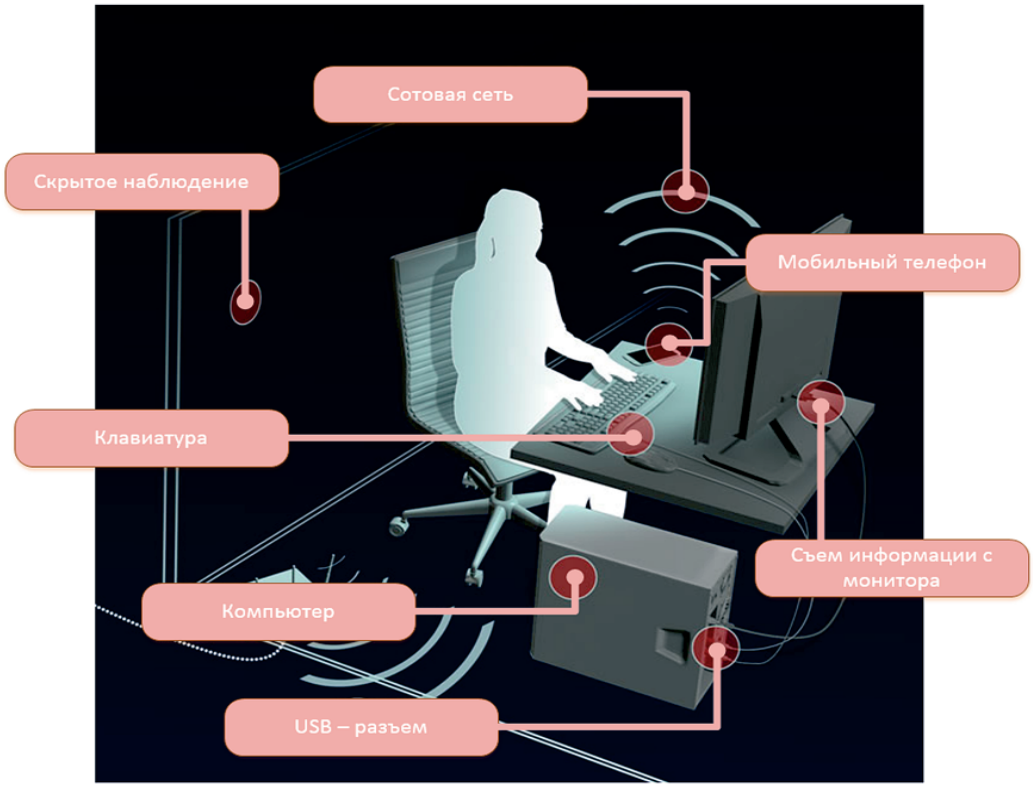
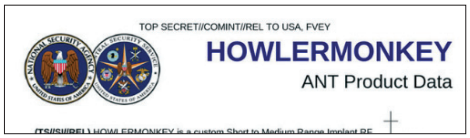


Рис. 2. *Потенциальная возможность установки закладок на оборудование рабочего места пользователя*

1. Компьютер

1.1. Системный блок



Закладка Howlermonkey представляет собой аппаратный радио-модуль, который в совокупности с другими элементами позволяет снимать удаленно данные с вычислительных компонент, а также осуществлять удаленное управление. Общий вид и размеры представлены на Рис. 3.

Рис. 3. *Закладка HOWLERMONKEY*

Закладка MAESTRO-II – это модуль на интегральных схемах, который может быть легко сконфигурирован для выполнения специальных задач. Общий вид и относительные размеры представлены на Рис. 4.

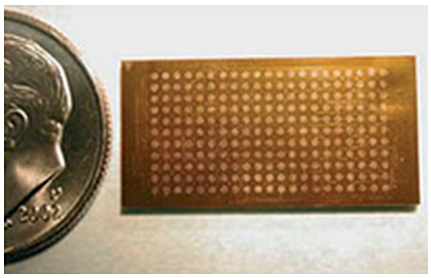
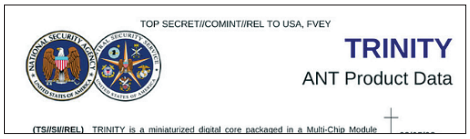


Рис. 4. *Закладка MAESTRO-II*



Закладка TRINITY – это модуль на интегральных схемах, который может быть использован, как имплант благодаря небольшим размерам (меньше монеты, стоимостью 1 цент – 2 см). Общий вид и относительные размеры представлены на Рис. 5.

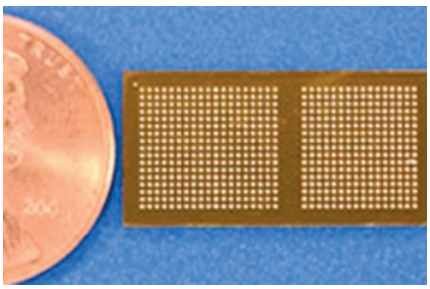


Рис. 5. *Закладка TRINITY*

Закладка GINSU – это программная часть комплекса, которая состоит из аппаратного импланта BULLDOZER (устанавливается в разъем PCI) и программной закладки KONGUR. В совокупности позволяет осуществлять удаленный доступ к Windows - системам.

Закладка IRATEMONK – представляет собой зловредный код в прошивке накопителей на жестких дисках от следующих производителей: Western Digital, Seagate, Maxtor and Samsung.

Он позволяет заменять MBR (Master Boot Record – загрузочная мастер-запись).

Закладка SWAP – представляет собой зловредный код в прошивке BIOS, который позволяет удаленное управление различных ОС (Windows, FreeBSD, Linux, Solaris) и файловых систем (FAT32, NTFS, EXT2, EXT3, UFS 1.0) на компьютере пользователя.

Закладка WISTFULTOLL – программная закладка для проведения атак несанкционированного доступа к данным используя протокол WMI (Windows Management Instrumentation). Также может быть использован как подключаемый модуль для программ-шпионов UNITEDDRAKE и STRAITBIZZARE.

Закладка JUNIORMINT – аппаратный модуль на интегральных схемах, который может быть гибко конфигурирован для различного использования.

Закладка SOMBERKNAVE – Программный шпион под ОС Windows XP, который использует не задействованные порты беспроводного подключения. В результате к компьютеру можно удаленно несанкционированно подключаться и управлять им.

1.2. Разъем типа USB

Закладка COTTONMOUTH-I – Аппаратная закладка для осуществления возможности перехвата передачи данных, установки программ-троянов и других несанкционированных действий. Содержит встроенный радиопередатчик. Также может взаимодействовать с другими имплантами серии COTTONMOUTH. Внешний вид представлен на Рис. 6.

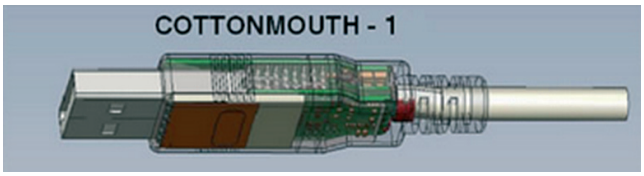


Рис. 6. *Аппаратный имплант COTTONMOUTH-1*

Закладка COTTONMOUTH-II – USB имплант, который позволяет проводить удаленное несанкционированное управление целевой системой. Подключается к другим модулям скрытых в шасси компьютера, что позволяет проводить подключения по радиоканалу. Внешний вид представлен на Рис. 7.

Рис. 7. *Аппаратный имплант COTTONMOUTH-II*

Закладка COTTONMOUTH-III – Представляет собой аппаратный USB имплант, который позволяет проводить скрытое подключение к компьютеру, даже если он выключен или недоступен по сетевым подключениям. Он подключается к другим закладкам, скрытым в шасси компьютера и позволяет проводить подключения по радиоканалу к оборудованию жертвы. Внешний вид представлен на Рис. 8.

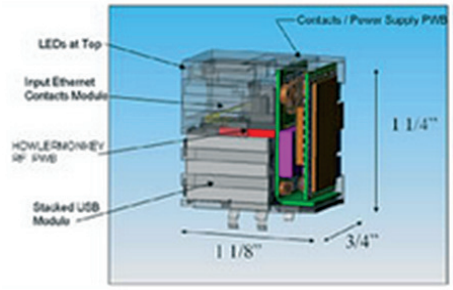


Рис. 8. *Аппаратный имплант COTTONMOUTH-III*

Закладка FIREWALK – Представляет собой аппаратный имплант в виде разъема типа Ethernet или USB. Позволяет проводить перехват данных и установку эксплоитов по радиоканалу. Внешний вид представлен на Рис. 9.

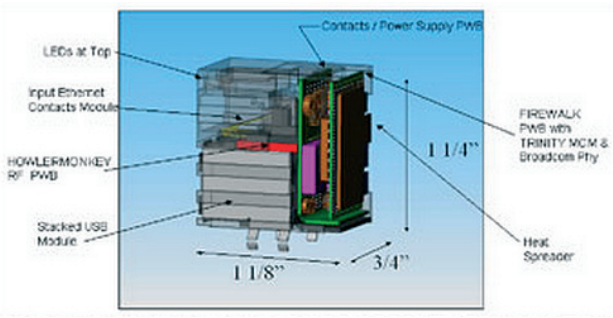


Рис. 9. *Аппаратный имплант FIREWALK*

1.3. Клавиатура

Закладка SURLYSPAWN – Задача установки программных регистраторов использования клавиатуры считается одной из простейших для спецслужб. Аппаратная закладка «SURLYSPAWN» еще более улучшает качество несанкционированного доступа с помощью возможности передачи даже когда компьютер не подключен к сети. Закладка излучает радио сигнал, который несет информацию о каждой нажатой клавиши. Данный радиосигнал может быть принят приемной станцией, которая находится вне здания. Это позволяет размещать агентов спецслужб в здании через улицу, при этом они будут знать, что печатается на компьютере, который даже не подключен к сети Интернет. Внешний вид представлен на Рис. 10.

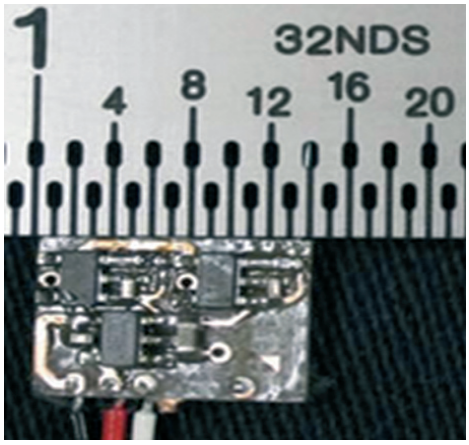


Рис. 10. Аппаратный имплант FIREWALK

1.4. Монитор

Закладка RAGEMASTER – Это аппаратная закладка для организации несанкционированной передачи видеосигнала с мониторов типа VGA. Работа закладки построена на пассивной основе, при этом передача информации осуществляется с помощью внешнего облучателя (радара). Имплант устанавливается в ферритовый фильтр, который находится на кабеле монитора. Внешний вид представлен на Рис. 11.

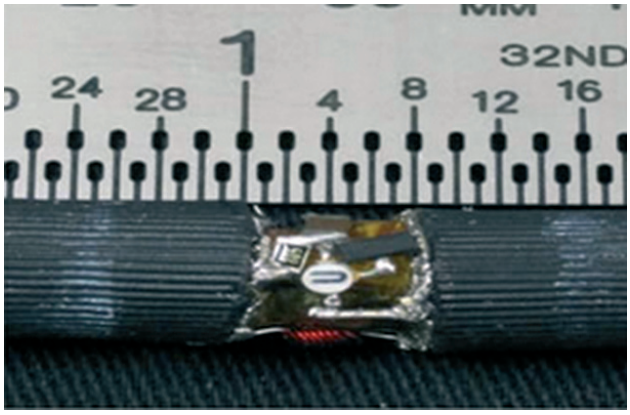


Рис. 11. Аппаратный имплант RAGEMASTER

2. Мобильная связь

2.1. Мобильный телефон

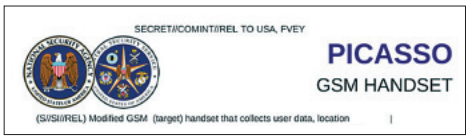
Закладка DROPOUTJEEP – Это программная закладка под операционную систему iOS для телефонов типа iPhone производства компании Apple. Закладка позволяет проводить несанкционированные удаленный доступ и управление с помощью SMS или сервисов обмена данными. Согласно документам АНБ, закладка обладает следующими возможностями: загрузка/выгрузка данных в/из телефона, просмотр адресной книги, прослушивание голосовых сообщений, определение местоположения телефона, включение микрофона или камеры без нотификации пользователя и определения сотовой сети. В начале 2008 года закладка находилась в стадии разработки.

Закладка GOPHERSET – закладка для GSM SIM карт, которая использует скрытую функциональность для доступа к адресной книге, SMS, журналу входящих/исходящих звонков.

Закладка MONKEYCALENDAR – закладка для SIM карты для несанкционированной передачи геоданных через скрытые текстовые сообщения SMS.

Закладка TOTECHASER – закладка, размещаемая в ПЗУ спутникового телефона Thuraya 2520, позволяет передавать данные из встроенной ОС Windows CE через скрытые текстовые сообщения SMS.

Закладка TOTEGHOSTLY – закладка из семейства STRAITBIZARRE, которая осуществляет полный контроль мобильных телефонов, которые работают под ОС Windows Mobile. Закладка обладает следующими возможностями: загрузка/выгрузка данных в/из телефона, просмотр адресной книги, прослушивание голосовых сообщений, чтение SMS сообщений, определение местоположения телефона, включение/выключение микрофона или камеры, определение базовой станции сотовой связи и т.д.



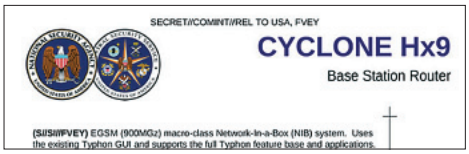
Закладка PICASSO – представляет собой серию модифицированных GSM телефонов, которые могут применяться для отслеживания местоположения или как подслушивающее устройство. Данные могут быть считаны через USB интерфейс или переданы через скрытые SMS сообщения.

2.2. Сотовая сеть

Закладка CROSSBEAM – представляет собой GSM модуль, который применяется в ноутбуках. Позволяет осуществлять перехват связи и проводить несанкционированное скрытое управление. Общий вид представлен на Рис. 12.

Рис. 12. *Аппаратная закладка CROSSBEAM*

CANDYGRAM – имитатор базовой GSM станции (диапазоны 900/1800/1900 МГц), который осуществляет определение физического размещения мобильного телефона жертвы и передает координаты через скрытые сообщения SMS.

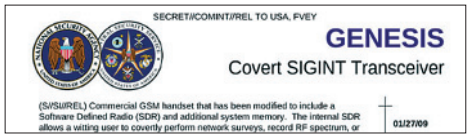


CYCLONE HX9 – имитатор базовой станции сети GSM, который позволяет проводить атаки на мобильные телефоны, работающие по протоколу GSM 900. Может использоваться для прослушивания и сбора данных мобильных телефонов. В частности, АБН подозревается в прослушке мобильного телефона канцлера Германии Ангелы Меркель (по данным журнала Spiegel). Общий вид устройства представлен на Рис. 13.

Рис. 13. *Имитатор CYCLONE HX9*

EBSR - имитатор базовой GSM станции (диапазоны 900/1800/1900 МГц), который позволяет проводить атаки мобильного телефона жертвы. Общий вид устройства представлен на Рис. 14

Рис. 14. *Имитатор EBSR*

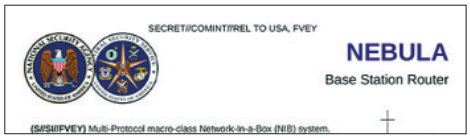


GENESIS – модифицированная версия обычного мобильного телефона для сетей GSM и 3G, который может определять характеристики и частотный спектр сотовой сети, а также обнаруживать мобильные телефоны. Общий вид телефона представлен на Рис. 15.

Рис. 15. *Модифицированный телефон GENESIS*

ENTOURAGE – аппаратный комплекс для «прямого поиска» мобильных телефонов, которые работают по стандарту GSM и 3G. Также может определять GPS координаты мобильного телефона. Общий вид устройства представлен на Рис. 16.

Рис. 16. *Устройство ENTOURAGE*



NEBULA – имитатор базовой станции для сетей 2G (900 МГц) и 3G (2100 МГц). Общий вид устройства представлен на Рис. 17.

Рис. 17. *Имитатор NEBULA*

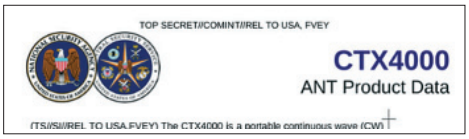
TYPHON HX – имитатор базовой станции (маршрутизатора), который поддерживает широко распространённые стандарты (850, 900, 1800, 1900 МГц). Позволяет осуществлять прослушивание мобильных телефонов. Общий вид устройства представлен на Рис. 18.

Рис. 18. *Имитатор TYPHON HX*

WATERWITCH – Устройство для точного отслеживания геолокации мобильных телефонов жертв, расположенных поблизости. Общий вид устройства представлен на Рис. 19.

Рис. 19. *Устройство WATERWITCH*

3. Скрытое наблюдение



Комплекс CTX400 – устройство облучения и приема волн от имплантов, например, семейства ANGRYNEIGHBOR. Является предшественником комплекса PHOTOANGLO. Среди других целей применения, использовался для сбора дан-

ных в рамках программы Dropmire. Программа Dropmire использовалась, в частности, против дипломатических представительств Европейского Союза в Вашингтоне, округ Колумбия. Общий вид комплекса представлен на Рис. 20.

Рис. 20. *Комплекс CTX400*

Закладка LOUDAUTO – является аппаратной закладкой в помещении, которая передает записанные переговоры по отраженной волне. Общий вид закладки представлен на Рис. 21.

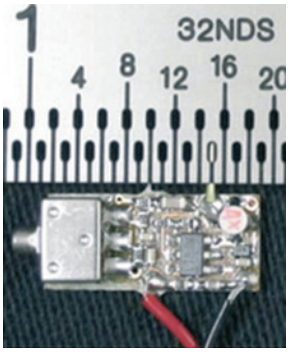
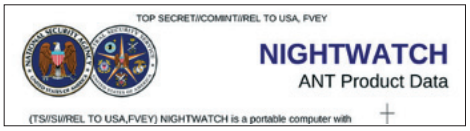
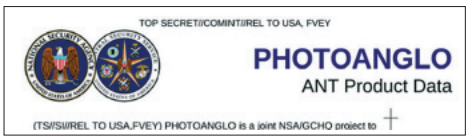


Рис. 21. *Закладка LOUDAUTO*



Монитор NIGHTWATCH – представляет собой систему, которая позволяет исследовать сигналы целевых систем. Общий вид комплекса представлен на Рис. 22.

Рис. 22. *Монитор NIGHTWATCH*



Система PHOTOANGLO – улучшенный радарный комплекс (пришедший на смену CTX4000) который обнаруживает отражения при непрерывном облучении (подсветки). Это позволяет принимать сигналы от закладных устройств, в частности типа ANGRYNEIGHBOR, на значительном расстоянии.

Закладка TAWDRYYARD – представляет собой аппаратный модуль, который отражает волны радара. Это позволяет определить его местоположение в помещении даже сквозь стены. Он может применяться, помимо других использований, для упрощения определения местоположения модулей RAGEMASTER (используются для перехвата сигналов от компьютерных мониторов). Общий вид комплекса представлен на Рис. 23.

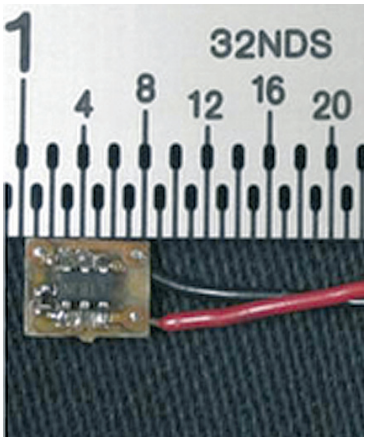


Рис. 23. *Закладка TAWDRYYARD*

4. Выводы

Полная классификация закладок по типу и применению представлена на рис. Рис. 24. Классификация закладок.

Системный подход по покрытию целевой инфраструктуры закладками на всех уровнях требует соответствующих системных мер по предотвращению и выявлению закладок. Под угрозой могут находится как конкретные устройства, так и каналы передачи данных. Знание типов закладок и принципов их работы позволяет выработать соответствующие ответные меры противодействия.

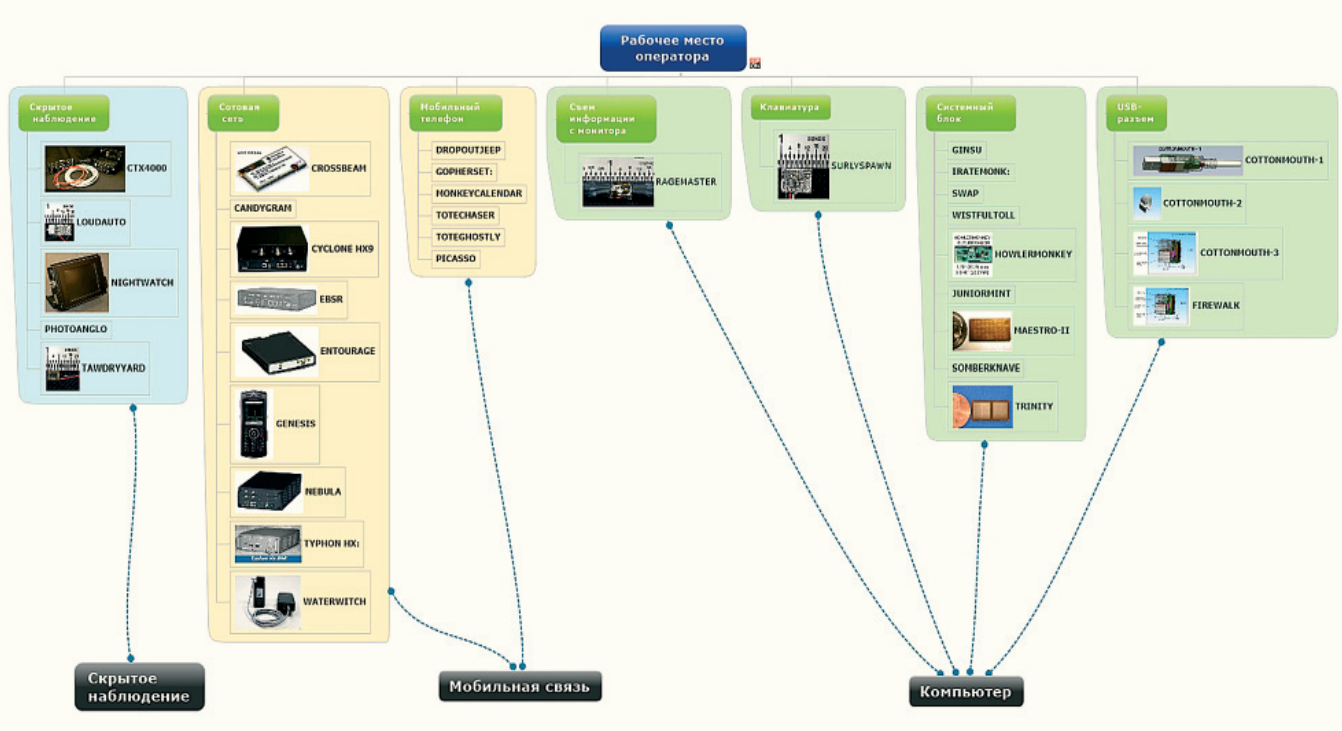


Рис. 24. Классификация закладок

Литература:

1. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. № 2 (3). С. 60-65.
2. Shopping for Spy Gear: Catalog Advertises NSA Toolbox. // Spiegel. 2014. URL: www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html .
3. Inside TAO: Documents Reveal Top NSA Hacking Unit. // Spiegel. 2014. URL: www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html .
4. Interactive Graphic: The NSA's Spy Catalog. // Spiegel. 2014. URL: www.spiegel.de/international/world/a-941262.html.
5. Марков А. С., Цирлов В. Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). С. 42-48.
6. Костогрызов А.И., Лазарев В.М., Любимов А.Е. Прогнозирование рисков для обеспечения эффективности информационной безопасности в их жизненном цикле // Правовая информатика. 2013. № 4. С. 4-16

References:

1. Klyanchin A. I. Katalog zakladok ANB (Spigel). Chast' 1. Infrastruktura, Voprosy kiberbezopasnosti (Cybersecurity issues), 2014, No 2 (3), pp. 60-65.
2. Shopping for Spy Gear: Catalog Advertises NSA Toolbox., Spiegel. 2014. URL: www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html .
3. Inside TAO: Documents Reveal Top NSA Hacking Unit., Spiegel. 2014. URL: www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html .
4. Interactive Graphic: The NSA's Spy Catalog., Spiegel. 2014. URL: www.spiegel.de/international/world/a-941262.html .
5. Markov A. S., Tsirlov V. L. Opyt vyyavleniya uyazvimostey v zarubezhnykh programmnykh produktakh, Voprosy kiberbezopasnosti (Cybersecurity issues), 2013, No 1 (1). pp. 42-48.
6. Kostogry`zov A.I., Lazarev V.M., Liubimov A.E. Prognozirovanie riskov dlia obespecheniia e`ffektivnosti informatcionnoi` bezopasnosti v ikh zhiznennom tcicle // Pravovaia informatika. 2013. № 4. S. 4-16