ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ ЗАЩИТЫ ОТ ЦЕЛЕВЫХ ВРЕДОНОСНЫХ ПРОГРАММ ТИПА STUXNET

***Марков Алексей Сергеевич**, кандидат технических наук, старший научный сотрудник, CISSP*

***Фадин Андрей Анатольевич**, CISSP*

Рассмотрены особенности целевых вредоносных программ (ЦВП). Приведены примеры, модель, факторы эксплуатации целевых вредоносных программ. Предложены организационно–технические меры по защите компьютерных ресурсов от целевых вредоносных программ в свете современной нормативно–методической базы.

***Ключевые слова:** вредоносные программы, вирусы, меры безопасности, механизмы безопасности, менеджмент информационной безопасности, кибербезопасность, кибероружие*

ORGANIZATIONAL AND TECHNICAL PROBLEMS OF PROTECTION AGAINSTTARGETED MALWARE SUCH AS STUXNET

***Alexey Markov** , Ph.D., Associate Professor, CISSP*

***Andrey Fadin**, CISSP*

The characteristics of the target of malware are considered. The examples, model, factors of operation of targeted malware are shown. The organizational and technical measures to protect the computer resources from targeted malware in light of the current regulatory basis are proposed.

***Keywords:** malware, viruses, security measures, security controls, information security management, cybersecurity , cyberweapons, Stuxnet, Flame, Duqu*

Введение

Как известно, 2010 год ознаменовал начало новой эпохи киберпротивоборства, касающегося использования вредоносных программ промышленного назначения класса Stuxnet.

Высокая эффективность решения задач по компрометации точечных IT-целей, технологическая сложность реализации подобных вредоносных программ обусловили необходимость поиска и разработки новых путей обеспечения безопасности ресурсов критических систем. Анализу этой проблемной ситуации с организационно-технической точки зрения посвящена данная статья.

Актуальность вредоносных программ

Кибервойны как форма проявления межгосударственного противостояния вошли в активную фазу в последнем десятилетии прошлого века (см. рис.1). При этом разведывательная и деструктивная составляющая компьютерных воздействий имели больше полуавтоматизированный характер, будь то демонстративные атаки на отказ в обслуживании, подмена сайтов или рассылка троянских почтовых приложений. Однако кибервойны вышли на новый уровень после публикации информации об успешном применении комплексных высокотехнологичных вредоносных программ, ориентированных на решение точечных задач информационного противоборства, в том числе в области АСУ ТП.

Указанные целенаправленные вредоносные программы (ЦВП) как вид кибероружия имеют следующие особенности:

- избирательность цели и действий,
- использование уязвимостей, в том числе уязвимостей 0-дня, закладок и скрытых каналов;
- маскировка, скрытность, криптозащита, самоликвидация;
- широкая функциональность в плане решения целевых задач;

Рис.1. *Исторические примеры кибервойн*

- гибкая система репродуцирования,
- инфраструктурная поддержка, обновление и управление,
- масштабируемость, наличие СУБД атак,
- высокое качество кода, обработка некорректных ситуаций.

Примеры наиболее публичных подобных вредоносных программ представлены на рис.2.

Рассмотрим наиболее интересные, на наш взгляд, публичные ЦВП.

Stuxnet как пример промышленного кибероружия

Stuxnet – первое широко известное вредоносное программное средство, имеющее точечную целевую функцию компрометации конкретной

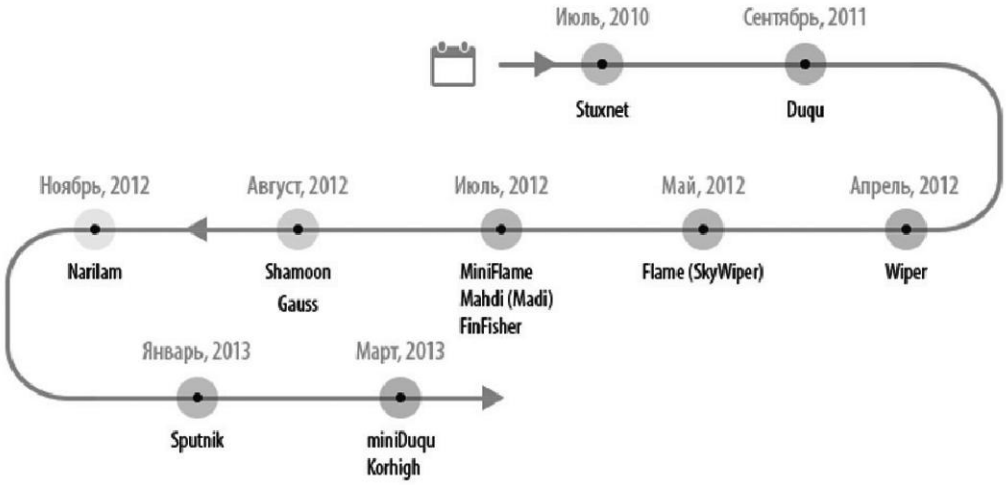

Рис. 2. *Лента сообщений об обнаружении фактов применения кибероружия*

конфигурации АСУ ТП.

Вредоносная программа Stuxnet была обнародована экспертом антивирусной компании «ВирусБлокАда» (Республика Беларусь). В настоящее время замечено несколько сотен тысяч заражений, около 60% из которых – на территории Ирана, причем деструктивные функции (модификация PLC-кода) реализованы строго избирательно. Активный период действия программы составляет 2009-2010 гг., однако были выявлены версии программы (Stuxnet 0.5), созданные, предположительно, в 2005 г. По заявлению бывших сотрудников NSA и JCS DoD, указанная вредоносная программа разработана в рамках американо-израильской операции противодействия ядерным планам Ирана.

Stuxnet включает десяток выполняемых компонент общим объемом в 1.2 Мб, написанных, главным образом, на языках C, C++ [1]. Базовой функциональной средой является Win32.

Отличительными особенностями Stuxnet являются:

- использование уязвимостей 0-дня;
- возможность распространения в изолированной среде (без выхода в Интернет), посредством flash-накопителей (flash-net) или собственной локальной p2p-сети;
- наличие компонент, подписанных похищенными 2-мя ЭЦП;
- заражение системы управления технологическими процессами Siemens Simatic Step7;
- выполнение модификации PLC-кода на контроллерах Siemens с целью деструктивного воздействия на физическое оборудование (ядерных центрифуг) и дезинформацию операторов завода.

Stuxnet поддерживает, как минимум, 8 способов репродуцирования, эксплуатацию более десяти уязвимостей, в том числе программной закладки (мастер-пароля), осуществляет контроль и управление через удаленные компьютеры (при обнаружении выхода в Интернет), включает Windows- и PLC-руткиты и другие способы маскировки и скрытия, также выполняет обработку ошибочных ситуаций и др. Stuxnet способен внедряться в ряд системных «доверенных» процессов, в том числе инициируемых антивирусными продуктами Avira, BitDefender, Computer Associates, Eset, F-Secure, Kaspersky Lab, McAfee, Symantec и Trend Micro.

В настоящее время описаны уязвимости, которые эксплуатировались разными релизами Stuxnet, а именно: CVE-2008-4250, CVE-2010-2549, CVE-2010-2568, CVE-2010-2719, CVE-2010-2729, CVE-2010-2743, CVE-2010-2744, CVE-2010-2772, CVE-2010-3338, CVE-2010-3888, CVE-2010-3889, CVE-2010-4252, CVE-2012-3015 и другие [1-4].

Flame как комплекс киберразведки

Вредоносная программа Flame, известная также как Skywiper или Flamer, является примером ЦВП, ориентированной на решение конкретных разведывательных задач на Ближнем Востоке, в первую очередь, в Иране. Flame был впервые описан учеными CrySyS (Венгрия) [5].

Замечено около 700 заражений. Активный период действия составляет порядка 6 лет до момента обнаружения.

Flame представляет собой комплекс программ объемом около 20 Мб (устанавливается поэтапно), в состав которого входят криптобиблиотеки, библиотеки архивирования, СУБД, веб-сервер, виртуальная машина. Базовой функциональной средой является Win32.

Ключевыми особенностями вредоносной программы являются:

- использование уязвимостей, в том числе 0-дня,
- компрометация ЭЦП (путем атаки на MD5),
- поиск офисных документов, проектной документации и чертежей (например, pdf и drw-файлов), контактной информации, в том числе из соцсетей,
- возможность перехвата аудио и экранной информации,
- поиск и подключение к Bluetooth-устройствам,
- закрытая передача информации на удалённый компьютер,
- наличие инструментария для взлома механизмов защиты.

Что касается последнего, то в составе имеются средства инвентаризации, мониторинга трафика, включая подсистему сбора парольной информации, поиска остаточной информации, анализа файловой системы, архивов и множества типов файлов, кейлогер и т.п.

Flame может распространяться через USB-носители и сеть, также имеет оригинальную возможность обновления путем компрометации Microsoft Windows Update.

К основным эксплуатируемым программой уязвимостям относят: CVE-2010-2568, CVE-2010-2729, CVE-2011-3402 [5,6].

Работа программы обеспечивается сложной динамичной инфраструктурой, например, известно около сотни доменов, задействованных для передачи данных на командные серверы Flame,

попеременно располагавшиеся в различных странах мира.

Несмотря на явно разведывательные цели, Flame содержит модуль удаления файлов.

Sputnik - троянская программа для кибершпионажа

Следует отметить, что для ряда вредоносных программ, а именно: Stuxnet, Flame, Duqu, Gauss, MiniFlame, MiniDuqu эксперты отмечают общие технологические черты, как-то: библиотеки (в том числе open source), среды, используемые уязвимости, приемы противодействия средствам защиты, а также качество кода и др. [7-9]. В то же время, среди ЦВП встречаются программы другой архитектуры, уровня технологичности, качества реализации.

Наглядным примером может быть троянская программа Sputnik, используемая в рамках разведывательной точечной кибероперации Red Ocrober. Целевой функцией троянской программы является сбор информации, касающейся деятельности дипломатических, правительственных, научных организаций. Максимальное число заражений пришлось на нашу страну. О факте проведения данной кибероперации сделали заявление специалисты Kaspersky Lab [10].

Особенностями указанной вредоносной программы являются:

- использование известных уязвимостей Windows-приложений (Word, Excel, Outlook) и механизма социальных атак,
- сбор нескольких десятков типов офисных, графических, почтовых, адресных файлов, в том числе уничтоженных,
- сбор данных со сменных носителей, дистанционных почтовых серверов и мобильных устройств (iPhone, Nokia, Windows Mobile),
- сбор параметров сетевых устройств,
- сложная распределенная система управления (около 60 доменов).

Отмечают такие особенности, как поддержка кириллицы и сбор файлов, закрытых с помощью Cryptofiler и PGP.

К основным эксплуатируемым программой уязвимостям относят: CVE-2009-3129, CVE-2010-3333, CVE-2012-0158.

Кибероперация Red Ocrober включает итерационные атаки с участием людей, когда в очередных атаках используются данные, полученные ранее.

Несмотря на то, что Sputnik не так технологически изящен, как кибероружие класса Stuxnet, указанное ЦВП встречается с 2007 года по сей день.

Факторы реализации вредоносных программ

Бытуют мифы, что противодействие вредоносным программам связано исключительно с использованием антивирусных средств, но, к сожалению, приведенные выше примеры демонстрируют обратное.

Можно назвать ряд технических факторов, из которых складывается успех современных ЦВП:

- наличие программных закладок, главным образом, мастер-паролей;
- наличие уязвимостей 0-дня;
- отсутствие своевременного закрытия известных уязвимостей;
- нарушения политик безопасности;
- другие факторы, связанные с недостаточностью традиционных мер защиты.

Часть угроз можно относительно легко исключить, а часть из них требует проведения серьезных тематических исследований.

Перечислим технические задачи противодействия эксплуатации ЦВП:

- выявление неизвестных дефектов безопасности программ путем аудита безопасности кода;
- сканирование известных уязвимостей;
- обновления с целью устранения уязвимостей, локализованных доверенными разработчиками систем,
- поиск и контроль активности известных классов компьютерных вирусов и других вредоносных программ,
- обнаружение вторжений в соответствии с базами сигнатур и паттернов;
- выявление нарушений информационных систем путем тестирования на проникновение,
- мониторинг событий безопасности в соответствии с сформулированными правилами и др.

Пример технических мер противодействия ЦВП приведен в табл.1.

Очевидно, что технические меры сами по себе не могут обеспечить необходимый уровень безопасности. Например, информирование и обучение сотрудников - важный фактор противодействия социальным атакам и обеспечения внимательности к угрозам.

Также важным моментом кибербезопасности является избирательность и уровень доверия к поставщикам ИТ-решений. Как известно, основным методом регулирования рынка ИБ является обязательная сертификация программного кода, когда испытательная лаборатория фиксирует исходные код и компоновочную среду, а в конечном счете – ответственность разработчика.

Таблица 1.
Примеры технических мер противодействия ЦВП

Негативный фактор	Защитные меры
Наличие уязвимостей 0-дня	Применение анализаторов кода Применение средств тестирования безопасности Применение SIEM-решений
Наличие известных уязвимости	Применение сканеров уязвимостей (VA), а также средств контроля обновлений («патчей») Внедрение политик по обновлению ПО Применение САВЗ, СОВ, SIEM
Установка в режимах небезопасной конфигурации	Применение сканеров уязвимостей, а также средств проверки конфигураций Внедрение политик по конфигурациям Применение СОВ, SIEM
Внедрение вредоносного ПО с помощью съемных носителей	Применение СЗИ от НСД Внедрение политик по работе со съемными носителями Применение САВЗ, SIEM
Внедрение вредоносного ПО с помощью методов социальной инженерии	Применение САВЗ, SIEM, систем фильтрации контента, DLP Внедрение политик по коммуникациям

Определение системного подхода

Как мы показали, исключительное использование традиционных антивирусных решений, основанных на сигнатурном поиске, не позволяет эффективно решать задачи защиты от ЦВП, т.е. необходим комплексный системный подход. Рассмотрим проблемную ситуацию на трех уровнях:

- нормативный уровень;
- уровень менеджмента;
- технический уровень.

Нормативный уровень

Если эволюция в области защиты информации конфиденциального характера очевидна, то нормативный комплекс по защите государственной тайны остается консервативным и ориентированным на директивные методы защиты, берущие начало еще от «Оранжевой книги» прошлого века (DoD 5200.28-STD: 1983). Фактически, такие защищенные системы предполагают наличие комплексных средств управления безопасным доступом (СВТ), дополненных средствами межсетевого управления доступом и антивирусными средствами. Несмотря на структурное единство и компактность указанных документов, надо понимать, что внедрение современных технологий связано с новыми классами угроз, в том числе угроз 0-дня.

Уровень менеджмента

Уровень менеджмента является самым важным в организации, т.к. на этом уровне уточняются задачи и требования, проводится управление рисками, формируются процедуры физического, технического и административного характера, включая работу с персоналом, что в итоге реализует весь жизненный цикл управления безопасностью информации организации, ее сегментов и подсистем [11].

Наиболее авторитетными в области менеджмента информационной безопасности считаются стандарты серии ISO 27000. Например, ISO/IEC 27001:2013 включает 114 механизмов (controls) безопасности, объединенных в 14 классов мер:

- политики информационной безопасности,
- организация информационной безопасности,
- безопасность персонала,
- управление ресурсами,
- контроль доступа,
- криптография,
- физическая безопасность и безопасность окружения,
- операционная безопасность,
- безопасность коммуникаций,
- безопасность поставки, разработки, сопровождения,
- связь с поставщикам,
- управление инцидентами информационной безопасности,
- управление непрерывностью бизнеса в плане информационной безопасности,
- соответствие нормативным требованиям.

Правильный выбор и реализация механизмов

безопасности определяют требуемый уровень защищенности от всевозможных актуальных угроз, в том числе связанных с вредоносными программами.

Технический уровень

В нашей стране, как известно, кроме средств криптографической защиты, нормативно пока определены средства защиты информации он несанкционированного доступа (СВТ), межсетевые экраны (МЭ), средства антивирусной защиты (САВЗ) и средства обнаружения вторжений (СОВ), но планируется расширение этого списка. В то же время ФСТЭК России сформулировала в ведомственном приказе № 17 (вступил в силу в сентябре 2013 г.) перечень организационно-технических мер защиты информации конфиденциального характера в государственных информационных системах, а именно [12]:

- идентификация и аутентификация,
- управление доступом,
- ограничение программной среды,
- защита машинных носителей информации,
- регистрация событий безопасности,
- антивирусная защита,
- обнаружение (предотвращение) вторжений,
- контроль (анализ) защищенности информации,
- целостность информационной системы и информации,
- доступность информации,
- защита среды виртуализации,
- защита технических средств,
- защита информационной системы и передачи данных.

Указанный перечень базовых мер можно использовать при формировании списка контрмер и средств защиты конкретной информационной системы.

Полученный список можно усиливать согласно модели актуальных угроз и дополнительных требований. К примеру, надо понимать, что уровень аудита безопасности кода, декларируемый в Приказах ФСТЭК России № 21 и 17, разумеется, недостаточен для выявления уязвимостей 0-дня, т.е. указанные требования следует поднять, как минимум, до 2-го уровня контроля отсутствия недекларированных возможностей (НДВ), который включает проверку конструкций кода.

Пример организации системы защиты от целевых вредоносных программ

Рассмотрим организацию защиты на примере Stuxnet. Схему работы ЦВП можно представить UML-диаграммой деятельности (см. рис1).

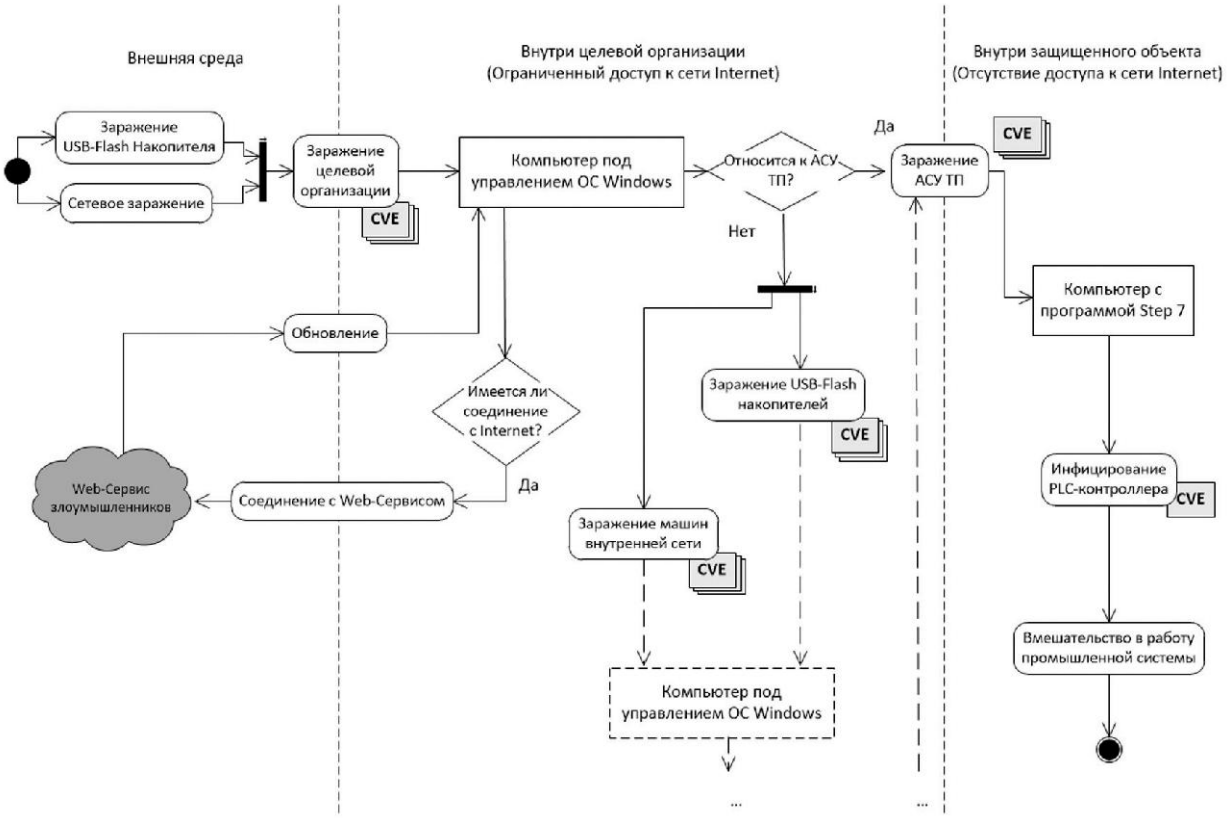

Рис. 3. *Общая схема функционирования Stuxnet*

На рисунке 3 показаны основные факторы эксплуатации ЦВП, связанные с наличием уязвимостей, что послужило главной причиной неэффективности используемых СЗИ.

В целях противодействия внедрению и работе ЦВП предлагается внедрение комплекса организационно-технических мер и процедур, часть из которых показана в табл. 2.

Опыт США в области кибербезопасности

Следует отметить несколько моментов из зарубежного опыта. К примеру, США - страна, находящаяся в состоянии жесткого противоборства с технологической экспансией со стороны Китая. Геополитические амбиции США определили несколько векторов развития стратегии кибербезопасности США:

- развитие научно-технического потенциала страны,
- создание и усиление кибервойск, сил и средств кибервооружений,
- смещение задач оценки соответствия от показателей «доверия» в направлении кибербезопасности путем обязательного проведения тестов на проникновение и аудита безопасности программного кода,
- ведение черных и белых списков поставщиков.

Особое внимание в США уделено обязательным системам менеджмента информационной безопасности федеральных служб в соответствии с актом FISMA-2002.

Таблица 2.

Примеры классов контрмер и средств защиты от ЦВП

Негативный фактор	ISO/IEC 27001:2013, механизмы безопасности	Приказ ФСТЭК России № 17, базовые меры
Уязвимости 0-дня	A.12.4. Регистрация и мониторинг A.16.1.4. Классификация событий A.14.2.8/9. Тестирование/испытания A.18.2.2/3. Оценка соответствия	РСБ.4/5 Регистрация событий ЗИС.16. Скрытые каналы ЗИС.27. Ложные системы ИАФ.7. Идентификация исполняемых модулей ОПС.4. Контроль временных файлов ОПС.1-3. Ограничения ПС **НДВ.2. Усиление в части НДВ-2**
Незакрытые известные уязвимости	A.12.6.1. Управление уязвимостями A.16.1.3. Оповещение о недостатках	АВЗ.2 Обновления САВЗ СОВ.2 Обновления СОВ АНЗ.1/2 Анализ уязвимостей
Скомпрометированный пароль	A.9.4.3. Системы управления паролями	АНЗ.5. Правила паролей
Идентифицируемый вредоносный код	A.12.2.1. Защита от вредоносных программ	АВЗ.1/2 Антивирусная защита
Зараженные съемные носители	A.6.2.1. Политика для мобильных устройств A.8.3.1. Управление съемными носителями	УПД.15 Мобильные средства ЗНИ.1-3.7. Носители информации
«Недоверенные» обновления	A.14.2.3/4. Тестирование/контроль изменений	АНЗ.2. Контроль обновлений
Раскрытие технологической конфигурации	A.13.2.4. Соглашения о неразглашении	ОЦЛ.5. Контроль контента ЗИС.28. Скрытие структуры ИС
Внешнее управление	A.13.1.3. Разделение сетей A.14.1.2. Защита от публичных сетей	УПД.16. Взаимодействие между системами

Заключение

Факты применения ЦВП демонстрируют новый технологический уровень информационного противоборства в киберпространстве. Очевидно, что в создание таких средств вовлечены чрезвычайно квалифицированные исследователи, разработчики и тестировщики, имеющие в том числе доступ к новейшим достижениям криптографии, ИТ и АСУ ТП [14-18].

Исследование указанных вредоносных программ произошло благодаря публичной деятельности экспертов зарубежных или международных антивирусных компаний и научных заведений [1-10].

Статистика многолетней скрытой активности указанных вредоносных программ продемонстрировала необходимость серьезного совершенствования подходов в области информационной безопасности. В частности, рекомендуется комплексное решение, сочетающее развитие нормативной базы, внедрение лучших практик менеджмента информационной безопасности, комплексов сертифицированных средств защиты информации, в первую очередь, средств тестирования систем защиты и мониторинга событий безопасности (VA- и SIEM-технологий).

С точки зрения кибербезопасности, первостепенные шаги следует сделать в направлении развития методологии, методов и средств тестирования на проникновение и аудита безопасности программного кода.

Литература

1. Larimer J. An inside look at Stuxnet // IBM X-Force. 2010. 37 p.
2. Byres E., Ginter A., Langill J. How Stuxnet Spreads. A Study of Infection Paths in Best Practice Systems // White paper by TS/AT/SH. 2011. 26 p.
3. Falliere N., Murchu L.O., Chien E. W32.Stuxnet Dossier // Symantec Security Response. 2011. 69 p.
4. Matrosov A., Rodionov E., Harley D., Malcho J. Stuxnet Under the Microscope // ESET. 2012. 85 p.
5. Skywiper: a complex malware for targeted attacks / by Skywiper Analysis Team // Technical Report by Laboratory of Cryptography and System Security. Budapest: Budapest University of Technology and Economics. 2012. 64 p.
6. Walter J. Flame attacks: briefing and compromise. // White paper by McAfee Labs. 2012. 14 p.
7. Chien E., OMurchu L., Falliere N. W32.Duqu. The precursor to the next Stuxnet // Symantec Security Response. 2011. 71 p.
8. Duqu: A Stuxnet-like malware found in the wild / B.Bencsáth, G.Pék, L.Buttyán, M.Félegyházi // Technical Report by Laboratory of Cryptography and System Security. Budapest: Budapest University of Technology and Economics. 2011. 60 p.
9. Gauss: Abnormal Distribution // Kaspersky Lab Global Research and Analysis Team. 2012. 48 p.
10. Гостев А.А. Операция Red October - обширная сеть кибершпионажа против дипломатических и государственных структур // Право и кибербезопасность. 2013. № 1. С. 15-23.
11. Дорофеев А.В., Шахалов И.Ю. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. С. 4-14.
12. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. ФСТЭК России. 2013. Рег.№ 28608. 37 с.
13. Организация антивирусной защиты: опыт МО США / А.С.Марков и С.А.Щербина // PC Week. 2007. №44 (602). С.17.
14. Кухаркин А.В. Киберугрозы и защита информации // Научно-аналитический журнал Обозреватель - Observer. 2012. Т. 273. № 10. С. 94-104.
15. Левыкин М.В. Новые особенности самораспространяющихся вредоносных программ // Системы и средства информатики. 2011. Т. 21. № 2. С. 69-72.
16. Симоненко М.Д. Stuxnet и ядерное обогащение режима международной информационной безопасности // Индекс безопасности. 2013. Т. 19. № 1. С. 233-248.
17. Тарасов А.М. Кибершпионы: Duqu, Stuxnet, Flame, Gauss: что дальше? // Право и кибербезопасность. 2012. № 1. С.23-26.
18. Фрейдман А.В. Stuxnet и промышленная безопасность. // Автоматизация в промышленности. 2011. № 11. С. 48-53.

References

1. Larimer J. An inside look at Stuxnet, IBM X-Force, 2010, pp. 1-37.
2. Byres E., Ginter A., Langill J. How Stuxnet Spreads. A Study of Infection Paths in Best Practice Systems, White paper by TS/AT/SH, 2011, pp. 1-26.
3. Falliere N., Murchu L.O., Chien E. W32.Stuxnet Dossier, Symantec Security Response, 2011, pp. 1-69.
4. Matrosov A., Rodionov E., Harley D., Malcho J. Stuxnet Under the Microscope, ESET, 2012, pp. 1-85.
5. (Skywiper: a complex malware for targeted attacks), Paper by Skywiper Analysis Team, Technical Report by Laboratory of Cryptography and System Security, Budapest, Budapest University of Technology and Economics, 2012, pp. 1-64.
6. Walter J. (Flame attacks: briefing and compromise), White paper by McAfee Labs, 2012, pp. 1-14.
7. Chien E., OMurchu L., Falliere N. W32.Duqu, The precursor to the next Stuxnet, Symantec Security Response, 2011, pp 1-71.
8. Duqu: A Stuxnet-like malware found in the wild. By B.Bencsáth, G.Pék, L.Buttyán, M.Félegyházi, Technical Report by Laboratory of Cryptography and System Security, Budapest, Budapest University of Technology and Economics, 2011, pp. 1-60.
9. Gauss: Abnormal Distribution, Kaspersky Lab Global Research and Analysis Team, 2012, pp. 1-48.
10. Gostev A.A. Operatsiya Red October - obshirnaya set kibershpionazha protiv diplomaticheskikh i gosudarstvennykh struktur, (Operation Red October - a vast network of cyber espionage against diplomatic and governmental structures), Pravo i kiberbezopasnost. 2013. № 1. pp. 15-23.
11. Dorofeyev A.V., Shakhalov I.Yu. Osnovy upravleniya informatsionnoy bezopasnostyu sovremennoy organizatsii, (The Basics of Information Security Management modern organization), Pravovaya informatika, 2013, pp. 4-14.
12. Trebovaniya o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh, (Requirements for protection of information that is not state secrets contained in public information systems), FSTEC Russia, 2013, Reg.№ 28608, pp. 1-37.
13. Markov A., Shcherbina S. Organizatsiya antivirusnoy zashchity: opyt DoD (The organization of anti-virus protection: the experience of the U.S. DoD), PC Week, R.Ed., 2007, No 44 (602), pp. 17-17.
14. Kukharkin A.V. Kiberugrozy i zashchita informatsii, (Cyberthreats and protection of information), Nauchno-analiticheskiy zhurnal Obozrevatel – Observer, 2012, Vol 273, No 10, pp. 94-104.
15. Levykin M.V. Novyye osobennosti samorasprostranyayushchikhsya vredonosnykh programm, (New features self-propagating malware), Sistemy i sredstva informatiki, 2011, Vol 21, No 2, pp. 69-72.
16. Simonenko M.D. Stuxnet i yadernoye obogashcheniye rezhima mezhdunarodnoy informatsionnoy bezopasnosti, (Stuxnet and nuclear enrichment regime of international information security), Indeks bezopasnosti, 2013, Vol 19, No 1, pp. 233-248.
17. Tarasov A.M. Kibershpiony: Duqu, Stuxnet, Flame, Gauss: chto dalshe? (Cyberspies: Duqu, Stuxnet, Flame, Gauss: what next ?), Pravo i kiberbezopasnost, 2012, No 1, pp. 23-26.
18. Freydman A.V. Stuxnet i promyshlennaya bezopasnost, (Stuxnet and industrial safety), Avtomatizatsiya v promyshlennosti, 2011, No 11, pp. 48-53.